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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet CD-DAR RFI	
Solicitation No. - N° de l'invitation W6369-20CY06/B	**Date** 2020-07-09
Client Reference No. - N° de référence du client W6369-20CY06	**GETS Ref. No. - N° de réf. de SEAG** PW-$$QE-049-27832
File No. - N° de dossier 049qe.W6369-20CY06	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2021-06-30**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☑	
Address Enquiries to: - Adresser toutes questions à: See herein	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone ( ) - ( )	**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

Demande de renseignements (DR)

CYBER DEFENCE – DECISION ANALYSIS AND RESPONSE

W6369-20-CY06/B

Table des matières

PARTIE I - INTRODUCTION

Renseignements généraux

Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) ont fortement investi dans des technologies qui ont radicalement augmenté la rapidité et la précision des opérations militaires modernes. La plupart de ces progrès incroyables en matière de capacité découlent de la dépendance à un cyberespace de plus en plus complexe. Pour s'acquitter de leurs principales responsabilités de défendre le Canada, de défendre l'Amérique du Nord et de contribuer à la paix et à la sécurité internationales, le MDN et les FAC doivent être une force militaire moderne efficace, agile, adaptée, bien formée et bien équipée, dotée des capacités essentielles et de la souplesse qui sont requises pour contrer les menaces traditionnelles et asymétriques, y compris les cyberattaques.

Le projet CD-DAR s'harmonise aux objectifs de l'initiative no 65 de Protection, Sécurité, Engagement: La politique de défense du Canada, qui cite l'engagement du MDN et des FAC à « améliorer les capacités cryptographiques, les capacités des opérations d'information et les cybercapacités, ce qui inclura des projets de cybersécurité et de connaissance de la situation, l'identification des cybermenaces et la réponse à celles-ci, ainsi que le développement de capacités pour mener des opérations d'information et des cyberopérations offensives militaires dans le but de cibler, d'exploiter, d'influencer et d'attaquer à l'appui des opérations militaires ».[1]

À l'appui de leur structure de commandement et de contrôle, le MDN et les FAC ont besoin de pouvoir surveiller et contrôler leur cyberespace afin qu'il reste défendable. À cette fin, le projet CD-DAR du programme de développement de la cyberforce du MDN et des FAC se concentre sur l'application de ces exigences. Le projet CD-DAR est l'unique résultat du regroupement des projets de sensibilisation à la cybersécurité (SC) et de cyberopérations défensives – aide à la décision (CD-AD).

Résumé du projet : Au moyen du projet CD-DAR, le MND et les FAC acquerront une solution de cyberdéfense (qui se traduit en capacités) dans le but d'améliorer l'aide à la décision en général et la sécurité du cyberespace du MDN et des FAC, y compris la capacité de détecter les menaces, de les analyser et d'y réagir. La capacité intégrée du projet CD-DAR doit fournir une analyse contextuelle fiable à l'appui des décisions et des mesures du MDN et des FAC à l'intérieur d'extensions et d'interfaces désignées du réseau de commandement ainsi que des systèmes du Réseau étendu de la Défense (RED) déployables. En fin de compte, la capacité du projet CD-DAR permettra à la cyberforce des FAC de défendre la liberté d'action et les intérêts des FAC dans le cyberespace à l'appui des missions et des opérations des FAC. Néanmoins, le projet CD-DAR doit être conçu pour permettre l'évolutivité vers d'autres environnements de réseau, selon les besoins.

Le projet en est actuellement à la phase de définition.

Objectif de la présente demande de renseignements (DR)

Services publics et Approvisionnement Canada (SPAC)[2] , au nom du ministère de la Défense nationale (MDN) et

[1] Initiative nº 65 de Protection, Sécurité, Engagement : La politique de défense du Canada.

[2] La dénomination sociale du Ministère est « ministère des Travaux publics et des Services gouvernementaux ». « Services publics et Approvisionnement Canada » et « SPAC », de même que « Travaux publics et Services gouvernementaux Canada » et « TPSGC » sont les appellations usuelles.

des Forces armées canadiennes (FAC), publie cette demande de renseignements (DR) pour informer l'industrie de l'état du projet CD-DAR et du processus d'acquisition, ainsi que pour solliciter les commentaires de l'industrie.

En particulier, le gouvernement du Canada a l'intention d'utiliser la DR pour publier et solliciter des commentaires sur une ébauche d'une invitation à se qualifier (ISQ) et les parties non classifiées d'une ébauche de demande de propositions (DP) et de la DP finale. Toutes les réponses de l'industrie seront examinées par le Canada. Lorsque possible, les commentaires et les questions de l'industrie ainsi que les réponses concernant l'ébauche d'ISQ, l'ébauche de DP non classifiée et la DP non classifiée seront publiés sur le site Achatsetventes.gc.ca en tant que modifications à cette DR. La DR restera active jusqu'à la date de clôture de la DP finale.

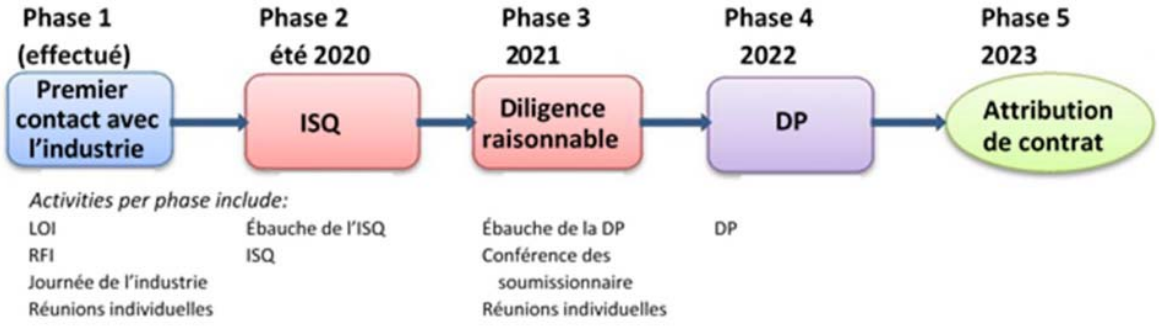
Pour encourager le plein accès de l'industrie et la transparence, l'ébauche d'ISQ, en plus d'être une annexe de cette DR, sera aussi publiée séparément sur Achatsetventes.gc.ca. L'ébauche de DP et la DP finale au complet, qui comprennent toutes deux des parties classifiées, seront fournies seulement aux fournisseurs qui se sont qualifiés au terme de l'ISQ. Les parties non classifiées de ces documents seront jointes en tant que modifications à cette DR à leur publication.

Aux fins de la DR, le terme « réponse » désigne toute question, tout commentaire, toute préoccupation, etc., communiqués à l'autorité contractante relativement aux documents ou au processus d'approvisionnement.

Résumé du processus d'approvisionnement prévu

La présente ISQ constitue la deuxième étape du processus d'approvisionnement du projet. Bien que le processus d'approvisionnement puisse être modifié (et même annulé, conformément aux instructions uniformisées de TPSGC), le Canada prévoit actuellement entreprendre le processus d'approvisionnement agile et collaboratif en plusieurs phases décrites ci-dessous.

CD-DAR - Processus d'approvisionnement prévu



Phase 1 – Premier contact avec l'industrie (effectué)

SPAC et le MDN ont commencé leurs efforts de sollicitation de l'industrie en publiant des lettres d'intérêt (LI) pour les projets de CD-AD et de SC en 2016, puis une demande de renseignements (DDR) en 2017. Une journée de l'industrie et des réunions individuelles classifiées ont eu lieu au printemps 2018. Cela a été fait dans le but d'obtenir une rétroaction sur les exigences opérationnelles et techniques, les coûts et le calendrier, et les retombées industrielles et technologiques. La rétroaction des fournisseurs découlant de ces efforts de sollicitation de l'industrie a été d'une grande utilité pour le Canada et a permis au MDN et aux FAC d'aller de l'avant avec le projet CD-DAR.

Phase 2 – Phase d'invitation à se qualifier

Ébauche de l'ISQ : La présente ébauche de l'ISQ marque le début de la deuxième phase de l'approvisionnement pour le projet CD-DAR. Les fournisseurs sont invités à soumettre des questions et des commentaires écrits sur cette ébauche de l'ISQ. Les questions et réponses seront affichées sur le site Achats et ventes.

ISQ officielle : L'ISQ servira à préqualifier les fournisseurs pour qu'ils puissent participer aux phases subséquentes de diligence raisonnable et de la DP et à toute autre phase potentielle du processus d'approvisionnement. Les fournisseurs sont invités à se soumettre à une sélection préalable, conformément aux modalités de la présente ISQ. Seuls les fournisseurs préqualifiés seront autorisés à soumissionner lors d'une demande de soumissions subséquente publiée dans le cadre du processus d'approvisionnement.

Phase 3 – Diligence raisonnable

SPAC ne mènera la phase de diligence raisonnable qu'avec les fournisseurs préqualifiés, comme déterminé dans la phase de qualification (Phase 2 – Phase d'invitation à se qualifier). L'objectif de la phase de diligence raisonnable est d'améliorer davantage les exigences du projet CD-DAR en obtenant des commentaires de la part de fournisseurs préqualifiés, en répondant aux préoccupations de l'industrie et en tenant compte des pratiques exemplaires de l'industrie avant de lancer la demande de soumissions finale. Les activités de la phase de diligence raisonnable sont les suivantes :

Ébauche de la DP : On s'attend à ce que les fournisseurs préqualifiés soient prêts à fournir de la rétroaction sur l'ébauche des documents de la DP, y compris les renseignements sur le système, l'ébauche de l'énoncé des besoins et l'ébauche des critères d'évaluation. Les éléments de l'ébauche de la DP sont classifiés et ne sont accessibles qu'aux fournisseurs préqualifiés qui satisfont aux exigences de sécurité de la DP. Les fournisseurs préqualifiés qui ne satisfont pas aux exigences de sécurité n'auront accès qu'aux éléments non classifiés de l'ébauche de la DP. Dans le cadre de cette DR, les parties non classifiées de l'ébauche de DP seront publiées sur le site Achatsetventes.gc.ca pour permettre aussi aux fournisseurs non qualifiés de fournir des commentaires. Le Canada examinera ces commentaires, y répondra lorsque possible et publiera les réponses dans une modification à cette DR.

Conférence des soumissionnaires classifiée et réunions individuelles classifiées avec des fournisseurs préqualifiés : Une conférence des soumissionnaires et des réunions individuelles avec des fournisseurs préqualifiés sont organisées pour discuter de questions précises concernant le contenu de l'ébauche des documents de la DP. De plus amples détails concernant la phase de diligence raisonnable sont fournis aux fournisseurs préqualifiés dans le cadre du processus de l'ébauche de la DP. Enfin, la finalisation de la DP tient compte de l'examen de la rétroaction de l'industrie après le processus de l'ébauche de la DP. La participation à la conférence des soumissionnaires classifiée et à la réunion individuelle classifiée n'est offerte qu'aux fournisseurs préqualifiés qui satisfont aux exigences de sécurité.

Phase 4 – Demande de propositions (DP)

SPAC prévoit publier une DP à l'intention des fournisseurs préqualifiés qui demeurent qualifiés au moment de la publication de la DP et qui satisfont aux exigences de sécurité de la DP décrites à l'annexe C. Si un fournisseur ne satisfait pas aux exigences de sécurité de la DP à la date d'émission de la DP, il sera retiré de la liste des fournisseurs préqualifiés. Les éléments non classifiés de la DP sont également publiés sur le site

Achats et ventes pour informer les fournisseurs non qualifiés. Lorsque possible, le Canada examinera les commentaires des fournisseurs non qualifiés et y répondra en publiant les réponses dans une modification à cette DR.

Phase 5 – Attribution du marché

PSPC anticipates awarding a contract to the winning supplier in accordance with the terms of the RFP.

PARTIE II - DEMANDE DE RENSEIGNEMENTS

1. Instructions pour répondre à cette demande de renseignements

1.1 Nature de la demande de renseignements

Cette occasion d'adresser des commentaires écrits au Canada en réponse à cette demande de renseignements (DR) et à tous les documents d'approvisionnement qui sont inclus ou peuvent l'être n'est PAS un appel d'offres ni une demande de propositions (DP) et ne doit être considérée d'aucune façon comme un engagement du Canada ou comme donnant le droit aux répondants potentiels d'entreprendre des travaux qui pourraient être facturés au Canada.

Cette DR ne fait PAS partie du processus d'acquisition officiel pour le projet CD-DAR, qui débutera quand l'ISQ finale sera publiée séparément sur Achatsetventes.gc.ca. Cette DR et tous les documents d'approvisionnement joints ne servent qu'à informer du processus les fournisseurs qui ne sont pas qualifiés au terme de l'ISQ et à leur demander des commentaires. Lorsque possible, le Canada examinera les commentaires des fournisseurs reçus dans le cadre de cette DR et publiera ses réponses, mais il n'est pas obligé de le faire.

Aux fins de la DR, le terme « réponse » désigne toute question, tout commentaire, toute préoccupation, etc., communiqués à l'autorité contractante relativement à l'ébauche d'ISQ, aux parties non classifiées de l'ébauche de DP et de la DP finale ou au processus d'approvisionnement. Aucune réponse officielle n'est exigée.

On rappelle aux répondants que ce document est une demande de renseignements et non une demande de propositions. Ainsi, les répondants sont invités à présenter leurs commentaires, leurs préoccupations, leurs recommandations et leurs questions concernant chaque document d'approvisionnement joint à la DR.

1.2 Nature et format des réponses demandées

Les fournisseurs peuvent fournir leur réponse de manière continue ou en une seule soumission pour n'importe quel document parmi l'ébauche d'ISQ, l'ébauche de DP et la DP finale, ou pour tous ces documents.

Les répondants doivent fournir leur réponse écrite concernant l'ébauche d'ISQ, l'ébauche de DP et la DP finale dans le cadre de cette DR au plus tard à la date et à l'heure indiquées sur la page Web principale de cette DR sur Achatsetventes.gc.ca. L'heure et la date de réponse seront modifiées chaque fois pour l'ébauche d'ISQ, l'ébauche de DP et la DP finale.

Pour faciliter l'examen des commentaires et pour qu'ils soient les plus utiles possible, le Canada demande que les répondants, le cas échéant, renvoient clairement dans leurs commentaires à la section de l'ébauche d'ISQ, de l'ébauche de DP et de la DP finale et mentionnent leur dénomination sociale complète ainsi que le nom, l'adresse, l'adresse courriel et le numéro de téléphone de leur personne-ressource.

Le Canada demande que les répondants soumettent leurs commentaires, leurs préoccupations, leurs recommandations et leurs questions par courriel à :

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

1.3 Exception au titre de la sécurité nationale

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

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

1.4 Demandes de renseignements

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

Autorité contractante primaire :
Laurie Stewart
Services publics et Approvisionnement Canada

Autorité contractante secondaire :
Patti Wight
Services publics et Approvisionnement Canada

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

1.5 Langue de la réponse

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

1.6 Surveillance de l'équité

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

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

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

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

2. Sécurité

Il n'y a aucune exigence de sécurité associée à la présente DR, mais il y a des exigences de sécurité associées à chaque phase du processus d'approvisionnement.

2.1 Exigences de sécurité associées aux activités d'approvisionnement

The Draft RFP, RFP and resulting contract each contain specific mandatory security requirements. Those Security Requirements will be detailed in the Security Requirements Annex of each of the Draft ITQ, ITQ, Unclassified Draft RFP and Unclassified RFP documents.

2.2 Marchandises contrôlées

L'ébauche de DP, la DP finale et le contrat subséquent exigeront l'accès à des marchandises contrôlées qui sont

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

3. Politique des retombées industrielles et technologiques (RIT)

La **Politique des retombées industrielles et technologiques (RIT)** s'appliquera au projet Cyberdéfense – Analyse des décisions et réponse (CD-ADR). En vertu de la Politique des RIT, les entreprises qui se voient attribuer des contrats d'approvisionnement en matière de défense sont tenues de mener des activités commerciales au Canada, dont la valeur équivaut à celle du contrat. La Politique des RIT comprend une proposition de valeur (PV) qui exige des soumissionnaires qu'ils se fassent concurrence sur la base des retombées économiques pour le Canada associées à chaque soumission. Les soumissionnaires retenus sont sélectionnés en fonction du prix, du mérite technique et de leur PV. Les engagements relatifs à la PV pris par le soumissionnaire retenu deviennent des obligations contractuelles dans le contrat subséquent. Afin d'optimiser l'impact économique qui peut être obtenu de la PV, le Canada cherchera à utiliser la Politique des RIT pour motiver les entrepreneurs à investir dans les Capacités industrielles clés (CIC), telles que la cyberrésilience et l'intelligence artificielle. En tant que technologies émergentes, ces CIC sont des domaines présentant un potentiel de croissance rapide et d'innovation. Par conséquent, le Canada cherchera à favoriser les débouchés dans ces technologies émergentes en motivant les partenariats et les investissements avec l'industrie et les établissements postsecondaires qui favorisent le développement des compétences et la recherche et le développement.

Le Canada collaborera avec des fournisseurs qualifiés à mesure que nous élaborerons les exigences de la proposition de valeur des RIT.

Pour de plus amples renseignements sur la Politique des RIT, y compris la PV, visitez la page http://www.canada.ca/rit.

ANNEXE A – ÉBAUCHE D'INVITATION À SE QUALIFIER

Projet Cyberdéfense - Décision, Analyse et Réponse (CD-DAR)

Ébauche d’invitation à se qualifier

Le présent préavis offre aux fournisseurs intéressés une occasion de soumettre une rétroaction écrite sur l'ébauche de l'invitation à se qualifier (ISQ) qui serait examinée par le Canada, avant la publication de la version finale de l'ISQ.

Cette occasion de fournir des commentaires écrits au Canada ne constitue ni un appel d’offres ni une demande de propositions; elle ne doit en aucun cas être considérée comme un engagement de la part du Canada, et elle n’autorise aucunement les éventuels répondants à entreprendre des travaux dont le coût pourrait être réclamé au Canada. La participation à la présente occasion de rétroaction écrite n’est ni une condition ni un préalable pour répondre à toute invitation à se qualifier subséquente.

Toutes les demandes de renseignements et autres communications relatives au présent avis, y compris la rétroaction sur l’ébauche d’invitation à se qualifier (ISQ), doivent être soumises par écrit à l’attention de l’autorité contractante de Services publics et Approvisionnement Canada, à l’adresse électronique du projet :

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

Les fournisseurs intéressés sont priés de fournir leurs commentaires le plus tôt possible. Les commentaires reçus après la date et l’heure de clôture pourraient ne pas être pris en compte.

Invitation à se qualifier

POUR

CYBERDÉFENSE - DÉCISION, ANALYSE ET RÉPONSE (CD-DAR)

ISQ NO, W6369-20-CY06/A

ébauche

Table des matières

ébauche

1. Renseignements généraux

1.1 Introduction

Objectif de la présente invitation à se qualifier (ISQ) : le projet Cyberdéfense – Décision, Analyse et Réponse (CD-DAR) est le regroupement des projets de sensibilisation à la cybersécurité (SC) et de cyberopérations défensives – aide à la décision (CD-AD). L'objectif de cette invitation à se qualifier (ISQ) émise par Services publics et Approvisionnement Canada (SPAC)[1] est de qualifier les fournisseurs qui sont en mesure de fournir une capacité CD-DAR pour entreprendre les étapes ultérieures du processus d'approvisionnement. Un aperçu plus détaillé du processus d'approvisionnement souple et collaboratif figure dans la section 1.3 et l'annexe E.

Le présent processus d'ISQ ne constitue pas une demande de soumissions ni un appel d'offres**.** Aucun contrat ne sera attribué à la suite des activités tenues pendant l'étape de l'ISQ. En tout temps pendant l'étape de l'ISQ, le Canada se réserve le droit d'annuler toute exigence de qualification incluse dans le projet. Étant donné que le Canada peut annuler le processus d'ISQ en totalité ou en partie, le processus d'approvisionnement subséquent décrit dans le présent document peut ne jamais avoir lieu. Les fournisseurs préqualifiés peuvent se retirer du processus d'approvisionnement à tout moment. Par conséquent, les fournisseurs préqualifiés peuvent décider de ne pas soumettre de proposition à une demande de soumission subséquente, quelle qu'elle soit.

1.2 Résumé du projet

a) **Renseignements généraux :** Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) ont fortement investi dans des technologies qui ont radicalement augmenté la rapidité et la précision des opérations militaires modernes. La plupart de ces progrès incroyables en matière de capacité découlent de la dépendance à un cyberespace de plus en plus complexe. Pour s'acquitter de leurs principales responsabilités de défendre le Canada, de défendre l'Amérique du Nord et de contribuer à la paix et à la sécurité internationales, le MDN et les FAC doivent être une force militaire moderne efficace, agile, adaptée, bien formée et bien équipée, dotée des capacités essentielles et de la souplesse qui sont requises pour contrer les menaces traditionnelles et asymétriques, y compris les cyberattaques.

Le projet CD-DAR s'harmonise aux objectifs de l'initiative no 65 de Protection, Sécurité, Engagement: La politique de défense du Canada, qui cite l'engagement du MDN et des FAC à « améliorer les capacités cryptographiques, les capacités des opérations d'information et les cybercapacités, ce qui inclura des projets de cybersécurité et de connaissance de la situation, l'identification des cybermenaces et la réponse à celles-ci, ainsi que le développement de capacités pour mener des opérations d'information et des cyberopérations offensives militaires dans le but de cibler, d'exploiter, d'influencer et d'attaquer à l'appui des opérations militaires ».[2]

[1] La dénomination sociale du Ministère est « ministère des Travaux publics et des Services gouvernementaux ». « Services publics et Approvisionnement Canada » et « SPAC », de même que « Travaux publics et Services gouvernementaux Canada » et « TPSGC » sont les appellations usuelles.

[2] Initiative nº 65 de Protection, Sécurité, Engagement : La politique de défense du Canada.

ébauche

À l'appui de leur structure de commandement et de contrôle, le MDN et les FAC ont besoin de pouvoir surveiller et contrôler leur cyberespace afin qu'il reste défendable. À cette fin, le projet CD-DAR du programme de développement de la cyberforce du MDN et des FAC se concentre sur l'application de ces exigences. Le projet CD-DAR est l'unique résultat du regroupement des projets de SC et de CD-AD.

b) **Résumé du projet :** Au moyen du projet CD-DAR, le MND et les FAC acquerront une solution de cyberdéfense (qui se traduit en capacités) dans le but d'améliorer l'aide à la décision en général et la sécurité du cyberespace du MDN et des FAC, y compris la capacité de détecter les menaces, de les analyser et d'y réagir. La capacité intégrée du projet CD-DAR doit fournir une analyse contextuelle fiable à l'appui des décisions et des mesures du MDN et des FAC à l'intérieur d'extensions et d'interfaces désignées du réseau de commandement ainsi que des systèmes du Réseau étendu de la Défense (RED) déployables. En fin de compte, la capacité du projet CD-DAR permettra à la cyberforce des FAC de défendre la liberté d'action et les intérêts des FAC dans le cyberespace à l'appui des missions et des opérations des FAC. Néanmoins, le projet CD-DAR doit être conçu pour permettre l'évolutivité vers d'autres environnements de réseau, selon les besoins.

Le projet en est actuellement à la phase de définition.

On trouve d'autres renseignements sur les exigences, les objectifs, les résultats et la portée du projet à l'annexe A : Énoncé des besoins opérationnels préliminaire. **Portée du processus d'approvisionnement prévu :**

i) **Clients potentiels :** La présente ISQ est publiée par SPAC. Il est prévu que le MDN utilise le ou les contrats résultant de toute demande de soumissions subséquente pour satisfaire aux exigences du projet CD-DAR.

ii) **Nombre de contrats :** SPAC envisage actuellement d'attribuer au moins un (1) contrat.

iii) **Durée du contrat :** SPAC détermine la durée de tout contrat subséquent et des options connexes une fois que l'approvisionnement progresse jusqu'à la phase de la demande de propositions (DP).

c) **Programme des marchandises contrôlées :** Ce marché est assujetti au Programme des marchandises contrôlées. La *Loi sur la production de défense* définit les marchandises canadiennes contrôlées comme étant certains biens énumérés dans la Liste des marchandises d'exportation contrôlée du Canada, un règlement établi en vertu de la *Loi sur les licences d'exportation et d'importation* (LLEI).

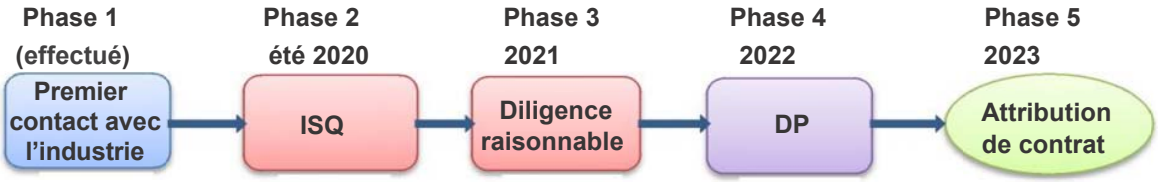
d) **Capacité financière :** La clause A9033T (2012-07-16) du Guide des clauses et conditions uniformisées d'achat (CCUA), Capacité financière, s'appliquera à la DP.

1.3 Résumé du processus d'approvisionnement prévu

La présente ISQ constitue la deuxième étape du processus d'approvisionnement du projet. Bien que le processus d'approvisionnement puisse être modifié (et même annulé, conformément aux instructions uniformisées de TPSGC), le Canada prévoit actuellement entreprendre le processus d'approvisionnement agile et collaboratif en plusieurs phases décrites ci-dessous.

ébauche

CD-DAR - Processus d'approvisionnement prévu



Activities per phase include:

LOI	Ébauche de l'ISQ	Ébauche de la DP	DP
RFI	ISQ	Conférence des soumissionnaire	
Journée de l'industrie			
Réunions individuelles		Réunions individuelles	

a) **Phase 1 – Premier contact avec l'industrie (effectué)**

SPAC et le MDN ont commencé leurs efforts de sollicitation de l'industrie en publiant des lettres d'intérêt (LI) pour les projets de CD-AD et de SC en 2016, puis une demande de renseignements (DDR) en 2017. Une journée de l'industrie et des réunions individuelles classifiées ont eu lieu au printemps 2018. Cela a été fait dans le but d'obtenir une rétroaction sur les exigences opérationnelles et techniques, les coûts et le calendrier, et les retombées industrielles et technologiques. La rétroaction des fournisseurs découlant de ces efforts de sollicitation de l'industrie a été d'une grande utilité pour le Canada et a permis au MDN et aux FAC d'aller de l'avant avec le projet CD-DAR.

b) **Phase 2 – Phase d'invitation à se qualifier**

Ébauche de l'ISQ : La présente ébauche de l'ISQ marque le début de la deuxième phase de l'approvisionnement pour le projet CD-DAR. Les fournisseurs sont invités à soumettre des questions et des commentaires écrits sur cette ébauche de l'ISQ. Les questions et réponses seront affichées sur le site Achats et ventes.

ISQ officielle : L'ISQ servira à préqualifier les fournisseurs pour qu'ils puissent participer aux phases subséquentes de diligence raisonnable et de la DP et à toute autre phase potentielle du processus d'approvisionnement. Les fournisseurs sont invités à se soumettre à une sélection préalable, conformément aux modalités de la présente ISQ. Seuls les fournisseurs préqualifiés seront autorisés à soumissionner lors d'une demande de soumissions subséquente publiée dans le cadre du processus d'approvisionnement.

c) **Phase 3 – Diligence raisonnable**

SPAC ne mènera la phase de diligence raisonnable qu'avec les fournisseurs préqualifiés, comme déterminé dans la phase de qualification (Phase 2 – Phase d'invitation à se qualifier). L'objectif de la phase de diligence raisonnable est d'améliorer davantage les exigences du projet CD-DAR en obtenant des commentaires de la part de fournisseurs préqualifiés, en répondant aux préoccupations de l'industrie et en tenant compte des pratiques exemplaires de l'industrie avant de lancer la demande de soumissions finale. Les activités de la phase de diligence raisonnable sont les suivantes :

ébauche

Ébauche de la DP : On s'attend à ce que les fournisseurs préqualifiés soient prêts à fournir de la rétroaction sur l'ébauche des documents de la DP, y compris les renseignements sur le système, l'ébauche de l'énoncé des besoins et l'ébauche des critères d'évaluation. Les éléments de l'ébauche de la DP sont classifiés et ne sont accessibles qu'aux fournisseurs préqualifiés qui satisfont aux exigences de sécurité de la DP décrites à l'annexe C. Les fournisseurs préqualifiés qui ne satisfont pas aux exigences de sécurité n'auront accès qu'aux éléments non classifiés de l'ébauche de la DP. Les éléments non classifiés de l'ébauche de la DP sont également publiés sur le site Achats et ventes afin de permettre aux fournisseurs non qualifiés de fournir des commentaires. Le Canada examine et répond à ces commentaires lorsque cela est possible et publie les résultats sur le site Achats et ventes.

Conférence des soumissionnaires classifiée et réunions individuelles classifiées avec des fournisseurs préqualifiés : Une conférence des soumissionnaires et des réunions individuelles avec des fournisseurs préqualifiés sont organisées pour discuter de questions précises concernant le contenu de l'ébauche des documents de la DP. De plus amples détails concernant la phase de diligence raisonnable sont fournis aux fournisseurs préqualifiés dans le cadre du processus de l'ébauche de la DP. Enfin, la finalisation de la DP tient compte de l'examen de la rétroaction de l'industrie après le processus de l'ébauche de la DP. La participation à la conférence des soumissionnaires classifiée et à la réunion individuelle classifiée n'est offerte qu'aux fournisseurs préqualifiés qui satisfont aux exigences de sécurité de la DP décrites à l'annexe C.

d) **Phase 4 – Demande de propositions (DP)**

SPAC prévoit publier une DP à l'intention des fournisseurs préqualifiés qui demeurent qualifiés au moment de la publication de la DP et qui satisfont aux exigences de sécurité de la DP décrites à l'annexe C. Si un fournisseur ne satisfait pas aux exigences de sécurité de la DP à la date d'émission de la DP, il sera retiré de la liste des fournisseurs préqualifiés. Les éléments non classifiés de la DP sont également publiés sur le site Achats et ventes pour informer les fournisseurs non qualifiés. Dans la mesure du possible, le Canada examine et répond aux commentaires des fournisseurs non qualifiés et publie les résultats sur le site Achats et ventes.

e) **Phase 5 – Attribution du marché**

SPAC prévoit attribuer un contrat au fournisseur retenu conformément aux modalités de la DP.

1.4 Compte rendu

L'autorité contractante avisera les fournisseurs non retenus après la phase de préqualification et leur fournira un compte rendu sur demande. Les fournisseurs non retenus devraient en faire la demande à l'autorité contractante dans les 15 jours ouvrables suivant la réception des résultats du processus de qualification. Le compte rendu peut être fourni par écrit, par téléphone ou en personne. L'autorité contractante doit déterminer quelle méthode sera la plus efficace.

1.5 Exceptions relatives à la sécurité nationale

Les exceptions relatives à la sécurité nationale prévues dans les accords commerciaux ont été invoquées; ce marché est donc entièrement exclu de l'ensemble des modalités de tous les accords commerciaux.

ébauche

1.6 Politique des retombées industrielles et technologiques (RIT)

La **Politique des retombées industrielles et technologiques (RIT)** s'appliquera au projet Cyberdéfense – Analyse des décisions et réponse (CD-ADR). En vertu de la Politique des RIT, les entreprises qui se voient attribuer des contrats d'approvisionnement en matière de défense sont tenues de mener des activités commerciales au Canada, dont la valeur équivaut à celle du contrat. La Politique des RIT comprend une proposition de valeur (PV) qui exige des soumissionnaires qu'ils se fassent concurrence sur la base des retombées économiques pour le Canada associées à chaque soumission. Les répondants retenus sont sélectionnés en fonction du prix, du mérite technique et de leur PV. Les engagements relatifs à la PV pris par le soumissionnaire retenu deviennent des obligations contractuelles dans le contrat subséquent. Afin d'optimiser l'impact économique qui peut être obtenu de la PV, le Canada cherchera à utiliser la Politique des RIT pour motiver les entrepreneurs à investir dans les Capacités industrielles clés (CIC), telles que la cyberrésilience et l'intelligence artificielle. En tant que technologies émergentes, ces CIC sont des domaines présentant un potentiel de croissance rapide et d'innovation. Par conséquent, le Canada cherchera à favoriser les débouchés dans ces technologies émergentes en motivant les partenariats et les investissements avec l'industrie et les établissements postsecondaires qui favorisent le développement des compétences et la recherche et le développement.

Le Canada collaborera avec des fournisseurs qualifiés à mesure que nous élaborerons les exigences de la proposition de valeur des RIT.

Pour de plus amples renseignements sur la Politique des RIT, y compris la PV, visitez la page http://www.canada.ca/rit.

1.7 Experts-conseils

a) Le Canada peut retenir les services d'experts-conseils dans le futur, à sa seule discrétion, pour les besoins du projet CD-DAR.

b) Le Canada transmettra aux experts-conseils, selon le besoin de savoir, les renseignements et les documents qui lui seront fournis, y compris ceux des fournisseurs préqualifiés, dans le cadre du processus d'approvisionnement.

c) Les experts-conseils sont tenus de signer un ou des accords de non-divulgation avant d'accéder à l'information et aux documents sur le Projet dans le cadre du présent processus d'approvisionnement.

1.8 Conflit d'intérêts ou avantage indu

Conformément aux dispositions des Instructions uniformisées – Biens ou services – Besoins concurrentiels 2003 (2020-05-28), une réponse peut être rejetée en raison d'un conflit d'intérêts réel ou apparent ou d'un avantage indu.

À cet égard, le Canada indique qu'il a eu recours aux services d'un certain nombre d'entrepreneurs du secteur privé dans la préparation des stratégies et des documents se rapportant à ce processus d'approvisionnement, y compris ceux qui suivent :

Entrepreneurs :

i. Modis Canada;

ébauche

ii. Veritaaq; and

iii. Procom.

Ressources (passé et présent) :

i. Marc Lessard;

ii. Paris Lampsos;

iii. Maurice Tremblay;

iv. Peter Ng; and

v. Stuart Morrison.

1.9 Surveillant de l'équité

Canada a fait appel aux services de *The Public Sector Company* comme surveillant de l'équité dans le cadre de cette acquisition. Le surveillant de l'équité observera, par exemple, l'évaluation des réponses afin de déterminer si SPAC a respecté le processus d'évaluation décrit dans la demande de soumissions. Selon son contrat avec le gouvernement du Canada, le surveillant de l'équité a l'obligation de préserver la confidentialité de tous les renseignements reçus dans le cadre de sa participation au présent processus d'approvisionnement.

ébauche

2. Instructions à l'intention des fournisseurs

2.1 Instructions, clauses et conditions uniformisées

a) Toutes les instructions, clauses et conditions définies par un numéro, une date et un titre dans l'ISQ sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditionsuniformisees-d-achat) publié par TPSGC.

b) Les fournisseurs qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la présente ISQ.

c) Le document 2003 (2020-05-28), Instructions uniformisées – Biens ou services – Besoins concurrentiels, est intégré par renvoi à l'ISQ et en fait partie intégrante, sauf dans les cas suivants :

   i) Chaque fois que le terme « demande de soumissions » est employé, il est remplacé par « invitation à se qualifier »;

   ii) Chaque fois que le terme « soumission » est employé, il est remplacé par « réponse »;

   iii) Chaque fois que le terme « soumissionnaire(s) » est employé, il est remplacé par « répondant(s) »;

d) La sous-section 5(4), qui traite de la période de validité, ne s'applique pas étant donné que l'ISQ invite les fournisseurs à se qualifier. À moins que le fournisseur n'informe l'autorité contractante de son désir de retirer sa réponse, le Canada supposera qu'il tient toujours à se qualifier.

e) Supprimer le paragraphe 01 – Dispositions relatives à l'intégrité – soumissions;

f) Supprimer le paragraphe 14 – Justification des prix;

g) Lorsqu'il soumet une réponse, le répondant s'engage à respecter les instructions, les clauses et les conditions de la présente ISQ.

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

2.2 Présentation d'une seule réponse

a) Un répondant peut être un particulier, une entreprise à propriétaire unique, une société commerciale, une société de personnes ou une coentreprise.

b) Chaque répondant (y compris les entités apparentées) ne pourra se qualifier qu'une seule fois. Si un répondant ou une entité apparentée participe à plusieurs réponses (participer signifie faire partie du répondant, et non pas être un sous-traitant), le gouvernement du Canada accordera deux (2) jours ouvrables à ces répondants pour indiquer la réponse unique que le gouvernement du Canada devra examiner. Si ce délai n'est pas respecté, toutes les réponses concernées pourraient être déclarées irrecevables ou le gouvernement du Canada pourrait choisir, à sa discrétion, les réponses qu'il évaluera.

c) Pour l'application du présent article, sans égard à la compétence où elle a été constituée en société ou formée juridiquement (qu'il s'agisse d'une personne, d'une société, d'une société de personnes, etc.), toute entité sera considérée comme « entité apparentée » d'un répondant :

ébauche

i) s'il s'agit de la même personne morale que le répondant (c.-à-d. la même personne physique, société commerciale, société de personne, société à responsabilité limitée, etc.);

ii) si l'entité et le répondant sont des « personnes liées » ou des « personnes affiliées » aux termes de la Loi de l'impôt sur le revenu du Canada;

iii) si l'entité et le répondant entretiennent une relation fiduciaire (découlant d'un arrangement entre agences ou toute autre forme de relation fiduciaire) ou ont entretenu une telle relation au cours des deux dernières années ayant précédé la clôture de l'ISQ;

iv) si l'entité et le répondant ont tout autre lien de dépendance entre eux, ou avec le même tiers.

d) Un répondant pourra agir en qualité de sous-traitant pour un autre répondant. Toutefois, les sous-traitants ne seront probablement pas autorisés à participer à l'étape de l'examen et de l'amélioration des exigences avec le répondant qualifié pour lequel ils exécutent un travail de sous-traitance.

e) Toute personne, entreprise individuelle, société, ou tout partenariat qui est un répondant dans le cadre d'une coentreprise ne peut soumettre une autre réponse de son propre chef ou sous l'égide d'une autre coentreprise, dans le cadre d'une même réponse.

Exemple 1 : Le fournisseur A, à lui seul, ne possède pas toute l'expérience requise par l'ISQ. Toutefois, le fournisseur B possède l'expérience qui manque au fournisseur A. Si les fournisseurs A et B décident de s'associer pour soumettre une réponse ensemble en tant que coentreprise, les deux entités seront considérées, ensemble, en tant que répondant. Les fournisseurs A et B ne peuvent pas s'associer avec un autre fournisseur pour soumettre une réponse distincte, parce qu'ils se sont associés pour former une coentreprise.

Exemple 2 : Le fournisseur X est un répondant. La filiale du fournisseur X, le fournisseur Y, décide de s'associer au fournisseur Z pour soumettre une réponse en tant que coentreprise. Les fournisseurs Y et Z, tout comme le fournisseur X, seront tous appelés à déterminer laquelle des deux réponses devra être prise en considération par le gouvernement du Canada. Les deux réponses ne peuvent pas être soumises, parce que le fournisseur Y est lié au fournisseur X en tant que société affiliée.

f) En soumettant une réponse, le répondant atteste qu'il ne se considère pas comme lié à tout autre répondant.

2.3 Lois applicables

L'ISQ sera interprétée et régie selon les lois en vigueur dans la province de l'Ontario, au Canada, et les relations entre les parties seront aussi régies par ces lois.

À leur discrétion, les répondants peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission ne soit mise en question, en supprimant le

ébauche

nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les répondants acceptent les lois applicables indiquées.

2.4 Questions, commentaires et communications

a) **Personne-ressource unique :** Afin d'assurer l'intégrité du processus d'approvisionnement concurrentiel, toutes les questions et autres communications ayant trait à l'ISQ doivent être adressées uniquement à l'autorité contractante.

Autorité contractante
Services publics et Approvisionnement Canada
Laurie Stewart
TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

b) **Date limite de soumission de questions :** À moins d'indication contraire dans l'ISQ, toutes les questions et observations à son sujet doivent être soumises par courriel à l'autorité contractante au plus tard cinq jours avant la date de clôture. Les questions reçues après cette date pourraient ne pas recevoir de réponse.

c) **Contenu des questions :** Les répondants doivent citer le plus fidèlement possible le numéro de l'article de l'ISQ auquel se rapporte la question. Ils doivent prendre soin d'énoncer chaque question de manière suffisamment détaillée pour permettre au gouvernement du Canada de fournir une réponse. Toute question qui comporte selon le répondant des renseignements exclusifs doit afficher clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments affichant la mention « exclusif » feront l'objet d'une discrétion absolue, à moins que le gouvernement du Canada considère que la question n'a pas un caractère exclusif. Le Canada peut modifier les questions ou peut demander au répondant de le faire, afin d'en éliminer le caractère exclusif et de permettre la transmission de la question modifiée et de la réponse à l'ensemble des répondants. Le gouvernement du Canada peut ne pas répondre aux questions dont la formulation ne permet pas de les transmettre à tous les répondants.

d) **Publication des réponses :** Pour garantir l'uniformité et la qualité des renseignements communiqués aux soumissionnaires, les questions importantes ainsi que les réponses seront publiées dans le Service électronique d'appels d'offres du gouvernement sous forme de modification à l'ISQ.

2.5 Droits du gouvernement du Canada

En plus de tout autre droit décrit dans l'ISQ, le gouvernement du Canada a le droit :

a) de modifier en tout temps la présente ISQ, y compris les critères de qualification;

b) d'annuler l'ISQ à n'importe quel moment;

c) de produire à nouveau l'ISQ;

d) si aucun répondant n'est qualifié et qu'aucune modification majeure n'a été apportée au besoin, de publier de nouveau la demande de soumissions en invitant uniquement les répondants qui ont

ébauche

soumissionné à soumissionner de nouveau, dans un délai indiqué par le gouvernement du Canada;

e) de rejeter et de ne pas examiner une réponse davantage si, à son avis, l'une des composantes de la réponse présente des questions ou des problèmes potentiels, perçus ou réels qui pourraient nuire à la sécurité nationale du Canada;

f) d'éliminer en tout temps tout répondant qualifié s'il présente des problèmes potentiels, perçus ou réels qui pourraient porter atteinte à la sécurité nationale du Canada;

g) à tout moment pendant la phase 3 – Diligence raisonnable, d'interrompre la phase 3 et de rouvrir la phase 2 – Phase d'ISQ.

2.6 Exigences en matière de sécurité

a) Au fur et à mesure que le projet CD-DAR progresse au cours des différentes phases d'approvisionnement, les exigences de sécurité évoluent et augmentent de beaucoup.

b) Le répondant n'est pas tenu d'avoir une autorisation de sécurité pour devenir un fournisseur préqualifié, mais des autorisations de sécurité et d'autres exigences de sécurité sont requises aux prochaines étapes du processus d'approvisionnement.

c) Afin d'être invités à la conférence des soumissionnaires (qui est le début de la phase de diligence raisonnable) et aux réunions individuelles classifiées, les fournisseurs préqualifiés doivent satisfaire aux exigences de sécurité décrites à l'annexe C, section 1.2 Exigences en matière de sécurité relatives à la phase 3 – Diligence raisonnable.

d) Lorsque le Canada est prêt à inviter des fournisseurs préqualifiés à la conférence des soumissionnaires et à une réunion individuelle classifiée (dates à déterminer), l'autorité contractante de SPAC communiquera avec le Programme de sécurité industrielle pour vérifier les autorisations de chaque fournisseur préqualifié. Les fournisseurs préqualifiés qui ne détiennent pas les autorisations appropriées à ce moment-là seront avisés qu'ils ne peuvent pas participer.

e) Il y aura des exigences de sécurité supplémentaires pour la DP définitive et le contrat. Les exigences de sécurité prévues pour la DP finale et le contrat sont également décrites à l'annexe C. Les fournisseurs préqualifiés qui ne satisfont pas aux exigences de sécurité pour la DP définitive, telles qu'elles sont décrites à l'annexe C, section 1.2, à la date de publication de la DP finale, seront retirés de la liste des fournisseurs préqualifiés.

Les fournisseurs préqualifiés qui ne détiennent pas actuellement les attestations de sécurité du personnel et les attestations de sécurité de l'organisation auprès du gouvernement fédéral canadien ou de leur programme national de sécurité industrielle respectif, ou encore, les fournisseurs qui ne respectent pas les exigences relatives à la sécurité prévues qui sont décrites à l'annexe C, doivent entreprendre tôt le processus d'obtention de l'attestation de sécurité en communiquant avec les responsables du Programme de la sécurité industrielle indiqué sur le site Web de TPSGC (https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html).

ébauche

3. Préparation et présentation de la réponse

3.1 Langue pour les communications à venir

Dans le formulaire de présentation de la réponse, chaque répondant doit indiquer dans laquelle des langues officielles du gouvernement du Canada il souhaite recevoir des communications futures de SPC à l'égard de son ISQ et tout au long du processus d'approvisionnement.

Si tous les fournisseurs admissibles aux termes de la présente ISQ choisissent la même langue officielle, le Canada peut décider de mener les prochaines étapes de communication et d'approvisionnement avec ces fournisseurs préqualifiés uniquement dans cette langue officielle.

3.2 Contenu de la réponse

Une réponse complète à la présente ISQ comprend tous les éléments décrits ci-après:

a) **Formulaire de présentation de la réponse (demandé à la clôture de l'ISQ) :** Les répondants doivent inclure dans leur réponse le formulaire de présentation de la réponse (Annexe D). Il s'agit d'un formulaire courant dans lequel les répondants peuvent fournir les renseignements exigés dans le cadre de l'évaluation, comme le nom d'une personne-ressource, le numéro d'entreprise – approvisionnement du répondant, la langue à utiliser lors des futures communications avec le gouvernement du Canada au sujet de ce processus d'approvisionnement, etc. L'utilisation de ce formulaire pour présenter les renseignements susmentionnés n'est pas obligatoire, mais recommandée. Si le gouvernement du Canada détermine que les renseignements exigés dans le formulaire de présentation de la réponse sont incomplets ou qu'ils doivent être corrigés, il accordera au répondant la possibilité de les compléter ou de les corriger. Pendant la période d'évaluation, il est obligatoire de fournir les renseignements sur demande.

b) **Réponses aux exigences de qualification de l'annexe B – Critères d'évaluation obligatoires (obligatoire à la clôture de l'ISQ) :** La réponse obligatoire du fournisseur doit justifier sa conformité aux critères obligatoires qui font l'objet d'une évaluation à l'annexe B – Critères d'évaluation obligatoires, et traiter ces critères de façon claire et suffisamment approfondie. Chaque critère d'évaluation obligatoire doit être traité avec suffisamment de détails pour permettre à l'équipe d'évaluation de vérifier la conformité du fournisseur. Il ne suffit pas de reprendre simplement les énoncés contenus dans l'ISQ. Afin de faciliter l'évaluation de la réponse, le gouvernement du Canada exige que les fournisseurs abordent et présentent les sujets dans le même ordre que les critères d'évaluation et sous le même titre. Pour éviter les recoupements, les répondants peuvent faire référence aux différentes sections de leur réponse en précisant l'article et le numéro de page où le sujet visé est déjà traité.

3.3 Présentation électronique d'une réponse

a) Les soumissions doivent être présentées uniquement au Module de réception des soumissions de Travaux publics et Services gouvernementaux Canada (TPSGC) au plus tard à la date et à l'heure indiquées à la page 1 de l'ISQ.

ébauche

b) Seules les soumissions présentées au moyen du service Connexion postel ou d'un télécopieur seront acceptées. Les soumissions sont closes au Module de réception des soumissions dans la région de la capitale nationale :

L'adresse courriel du Module de réception des soumissions est : À fournir dans l'ISQ officielle

Remarque : les soumissions envoyées directement à cette adresse courriel ne seront pas acceptées. Cette adresse de courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel qu'indiqué dans les instructions uniformisées 2003 ou pour envoyer des soumissions au moyen d'un message Connexion postel si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postel.

Le numéro de télécopieur du Module de réception des soumissions est : À fournir dans l'ISQ officielle

c) Il incombe au soumissionnaire de s'assurer que la demande d'ouverture d'une conversation Connexion postel est envoyée à l'adresse électronique ci-dessus au moins six jours civils avant la date de clôture de l'ISQ.

d) Le Canada demande au répondant de présenter sa soumission conformément à l'article 08 des instructions uniformisées de 2003. Le répondant doit transmettre sa soumission dans un seul envoi. Le service Connexion postel a la capacité de recevoir plusieurs documents, jusqu'à 1 Go par pièce jointe individuelle.

e) Si le répondant fournit simultanément plusieurs copies de sa soumission à l'aide de méthodes de livraison acceptable, et en cas d'incompatibilité entre le libellé de la copie électronique transmise par le service Connexion postel, le libellé de la copie électronique transmise par le service Connexion postel aura préséance sur le libellé des autres copies.

Les soumissions présentées au format papier à TPSGC ne seront pas acceptées.

ébauche

4. Processus d'évaluation des réponses

4.1 Évaluation des qualifications du répondant

Le gouvernement du Canada évaluera chacune des réponses afin de déterminer si elles satisfont à toutes les exigences obligatoires décrites dans la présente ISQ. Les dispositions relatives à l'évaluation comprises dans les Instructions uniformisées - biens ou services - besoins concurrentiels 2003 (2020-05-28) de TPSGC s'appliquent également. La réponse doit respecter toutes les exigences de l'ISQ pour être déclarée conforme.

4.2 Procédures d'évaluation

a) **Évaluation des réponses :** les réponses seront évaluées conformément aux exigences décrites dans la présente ISQ, y compris les exigences de qualification obligatoires de l'annexe B – Critères d'évaluation obligatoires.

b) **Équipe d'évaluation :** Les réponses seront évaluées par une équipe d'évaluation constituée de représentants du Canada. L'État peut faire appel à des experts-conseils ou à des personnes-ressources du gouvernement pour évaluer les réponses. Chaque membre de l'équipe chargée de l'évaluation ne participera pas nécessairement à tous les aspects de l'évaluation

c) D**emandes de précisions :** Si le Canada demande des précisions concernant une réponse ou s'il veut vérifier celle-ci, y compris les attestations, les répondants disposeront d'un délai de sept jours ouvrables (ou d'un délai plus long précisé par écrit par l'autorité contractante) pour fournir les renseignements nécessaires au Canada.

Selon la nature de la demande, le non-respect de ce délai peut entraîner le rejet de la réponse.

d) Pr**olongation de délai : Si le répondant a besoin de plus de temps, l'autorité contractante, à sa discrétion, peut accorder une prolongation du délai.**

4.3 Processus de conformité des soumissions en phase (PCSP)

(2018-07-19) Généralités

a) Pour ce besoin, le Canada applique le PCSP tel que décrit ci-dessous.

b) Nonobstant tout examen par le Canada aux phases I ou II du Processus, les répondants sont et demeureront les seuls et uniques responsables de l'exactitude, de l'uniformité et de l'exhaustivité de leurs soumissions, et le Canada n'assume, en vertu de cet examen, aucune obligation ni de responsabilité envers les répondants de relever, en tout ou en partie, toute erreur ou toute omission, dans les soumissions ou en réponse à toute communication provenant d'un répondant.

LE RÉPONDANT RECONNAÎT QUE LES EXAMENS LORS DES PHASES I ET II DU PRÉSENT PROCESSUS NE SONT QUE PRÉLIMINAIRES ET N'EMPÊCHENT PAS QU'UNE SOUMISSION SOIT NÉANMOINS JUGÉE NON RECEVABLE À LA PHASE III, ET CE, MÊME POUR LES EXIGENCES OBLIGATOIRES QUI ONT FAIT L'OBJET D'UN EXAMEN AUX PHASES I OU II, ET MÊME SI LA SOUMISSION AURAIT ÉTÉ JUGÉE RECEVABLE À UNE PHASE ANTÉRIEURE. LE

ébauche

CANADA PEUT DÉTERMINER À SA DISCRÉTION QU'UNE SOUMISSION NE RÉPOND PAS À UNE EXIGENCE OBLIGATOIRE À N'IMPORTE QUELLE DE CES PHASES. LE RÉPONDANT RECONNAÎT ÉGALEMENT QUE MALGRÉ LE FAIT QU'IL AIT FOURNI UNE RÉPONSE À UN AVIS OU À UN RAPPORT D'ÉVALUATION DE LA CONFORMITÉ (REC) (TEL QUE CES TERMES SONT DÉFINIS PLUS BAS) QU'IL EST POSSIBLE QUE CETTE RÉPONSE NE SUFFISE PAS POUR QUE SA SOUMISSION SOIT JUGÉE CONFORME AUX AUTRES EXIGENCES OBLIGATOIRES. (c)

(c) Le Canada peut, à sa propre discrétion et à tout moment, demander et recevoir de l'information de la part du soumissionnaire afin de corriger des erreurs ou des lacunes administratives dans sa soumission, et cette nouvelle information fera partie intégrante de sa soumission. Ces erreurs pourraient être, entre autres : une signature absente; une case non cochée dans un formulaire; une erreur de forme; l'omission d'un accusé de réception, du numéro d'entreprise d'approvisionnement ou même les coordonnées des personnes-ressources, c'est-à-dire leurs noms, leurs adresses et les numéros de téléphone; ou encore des erreurs d'inattention dans les calculs ou dans les nombres, et des erreurs qui n'affectent en rien les montants que le répondant a indiqué pour le prix ou pour tout composant du prix. Ainsi, le Canada a le droit de demander ou de recevoir toute information après la date de clôture de l'invitation à soumissionner uniquement lorsque l'invitation à soumissionner permet ce droit expressément. Le répondant disposera alors d'un délai indiqué pour fournir l'information requise. Toute information fournie hors délais sera refusée.

(d) Le PCSP ne limite pas les droits du Canada en vertu du Guide des clauses et conditions uniformisées d'achat (CCUA) 2003 (2020-05-28) Instructions uniformisées – biens ou services – besoins concurrentiels, ni le droit du Canada de demander ou d'accepter toute information pendant la période de soumission ou après la clôture de cette dernière, lorsque la demande de soumissions confère expressément ce droit au Canada, ou dans les circonstances décrites au paragraphe (c).

(e) Le Canada enverra un Avis ou un REC selon la méthode de son choix et à sa discrétion absolue. Le répondant doit soumettre sa réponse par la méthode stipulée dans l'Avis ou le REC. Les réponses sont réputées avoir été reçues par le Canada à la date et à l'heure qu'elles ont été livrées au Canada par la méthode indiquée dans l'Avis ou le REC et à l'adresse qui y figure. Un courriel de réponse autorisé dans l'Avis ou le REC est réputé reçu par le Canada à la date et à l'heure auxquelles il a été reçu dans la boîte de réception de l'adresse électronique indiquée dans l'Avis ou le REC. Un Avis, ou un REC, envoyé par le Canada au soumissionnaire à l'adresse fournie par celui-ci dans la soumission ou après l'envoi de celle-ci est réputé avoir été reçu par le répondant à la date à laquelle il a été envoyé par le Canada. Le Canada n'assume aucune responsabilité envers les répondants pours les soumissions retardataires, peu importe la cause.

Phase I: Soumission financière – Pas applicable

Phase II: Soumission technique

a) L'examen par le Canada au cours de la phase II se limitera à une évaluation de la soumission technique afin de vérifier si le répondant a respecté toutes les exigences obligatoires d'admissibilité. Cet examen n'évalue pas si la soumission technique répond à une norme ou répond à toutes les exigences de la soumission. Les exigences obligatoires d'admissibilité sont les critères techniques obligatoires tels qu'ainsi décrits dans la présente demande de soumissions comme faisant partie du

épuré

Processus de conformité des soumissions en phases. Les critères techniques obligatoires qui ne sont pas identifiés dans la demande de soumissions comme faisant partie du PCSP ne seront pas évalués avant la phase III.

b) Le Canada enverra un avis écrit au soumissionnaire REC précisant les exigences obligatoires d'admissibilité que la soumission n'a pas respectée. Un soumissionnaire dont la soumission a été jugée recevable au regard des exigences examinées au cours de la phase II recevra un REC qui précisera que sa soumission a été jugée recevable au regard des exigences examinées au cours de la phase II. Le répondant en question ne sera pas autorisé à soumettre des informations supplémentaires en réponse au REC.

c) Le répondant disposera de la période de temps précisée dans le REC (« période de grâce ») pour remédier à l'omission de répondre à l'une ou l'autre des exigences obligatoires d'admissibilité inscrites dans le REC en fournissant au Canada, par écrit, des informations supplémentaires ou des clarifications en réponse au REC. Les réponses reçues après la fin de la période de grâce ne seront pas prises en considération par le canada sauf, dans les circonstances et conditions expressément prévues par le REC.

d) La réponse du soumissionnaire doit adresser uniquement les exigences obligatoires d'admissibilité énumérées dans le rapport d'évaluation de conformité (REC) et considérées comme non accomplies, et doit inclure uniquement les renseignements nécessaires pour ainsi se conformer aux exigences. Toutefois, dans le cas où une réponse aux exigences obligatoires d'admissibilité énumérées dans le REC entraînera nécessairement la modification d'autres renseignements qui sont déjà présents dans la soumission, les rajustements nécessaires devront être mis en évidence par le répondant. La réponse au REC ne doit pas inclure de changement à la soumission financière. Toute autre information supplémentaire qui n'est pas requise pour se conformer aux exigences ne sera pas prise en considération par le Canada.

e) La réponse du soumissionnaire au REC devra spécifier, pour chaque cas, l'exigence obligatoire d'admissibilité du REC à laquelle elle répond, notamment en identifiant le changement effectué dans la section correspondante de la soumission initiale, et en identifiant dans la soumission initiale les modifications nécessaires qui en découlent. Pour chaque modification découlant de la réponse aux exigences obligatoires d'admissibilité énumérées dans le REC, le répondant doit expliquer pourquoi une telle modification est nécessaire. Il n'incombe pas au Canada de réviser la soumission du soumissionnaire; il incombe plutôt au soumissionnaire d'assumer les conséquences si sa réponse au REC n'est pas effectuée conformément au présent paragraphe. Toutes les informations fournies doivent satisfaire aux exigences de la demande de soumissions.

f) Tout changement apporté à la soumission par le répondant en dehors de ce qui est demandé, sera considéré comme étant de l'information nouvelle et ne sera pas prise en considération. L'information soumise selon les exigences de cette demande de soumissions en réponse au REC remplacera, intégralement et uniquement la partie de la soumission originale telle qu'elle est autorisée dans cette section.

g) Les informations supplémentaires soumises pendant la phase II et permises par la présente section seront considérées comme faisant partie de la soumission et seront prises en compte par le Canada

ébauche

dans l'évaluation de la soumission lors de la phase II que pour déterminer si la soumission respecte les exigences obligatoires admissibles. Celles-ci ne seront utilisées à aucune autre phase de l'évaluation pour augmenter les notes que la soumission originale pourrait obtenir sans les avantages de telles informations additionnelles. Par exemple, un critère obligatoire admissible qui exige l'obtention d'un nombre minimum de points pour être considéré conforme sera évalué à la phase II afin de déterminer si cette note minimum obligatoire aurait été obtenue si le répondant n'avait pas soumis les renseignements supplémentaires en réponse au REC. Dans ce cas, la soumission sera considérée comme étant conforme par rapport à ce critère obligatoire admissible et les renseignements supplémentaires soumis par le répondant lieront le répondant dans le cadre de sa soumission, mais la note originale du soumissionnaire, qui était inférieure à la note minimum obligatoire pour ce critère obligatoire admissible, ne changera pas, et c'est cette note originale qui sera utilisée pour calculer les notes pour la soumission.

h) Le Canada déterminera si la soumission est recevable pour les exigences examinées à la phase II, en tenant compte de l'information supplémentaire ou de la clarification fournie par le répondant conformément à la présente section. Si la soumission n'est pas jugée recevable selon des exigences examinées à la phase II à la satisfaction du Canada, la soumission financière sera jugée non recevable et rejetée.

i) Uniquement les soumissions jugées recevables selon les exigences examinées à la phase II et à la satisfaction du Canada seront ensuite évaluées à la phase III.

4.3 Critères de qualification de base

a) Lorsque la réponse

   i. respecter toutes les exigences de la ISQ; et

   ii. satisfaire à tous les critères d'évaluation techniques obligatoires à l'Annexe B;

   deviendra un fournisseur préqualifié pour la prochaine phase du processus d'approvisionnement

b) Le gouvernement du Canada se réserve le droit de réévaluer la qualification de tout répondant qualifié, et ce, à tout moment durant le processus d'approvisionnement. Par exemple, dans une situation où une attestation de sécurité en particulier est une des exigences de l'ISQ et que celle du répondant change ou vient à échéance, le gouvernement du Canada pourrait disqualifier ce répondant qualifié, étant donné qu'il ne répond plus aux exigences de l'ISQ. De même, si des informations sont signalées au Canada et qu'elles mettent en question les qualifications du répondant qualifié dans le cadre de la présente ISQ, le Canada peut évaluer de nouveau ce répondant. Le cas échéant, il pourrait demander plus d'information. Si le répondant qualifié ne les fournit pas dans les cinq (5) jours ouvrables (ou plus longtemps, selon l'autorité contractante), le Canada peut disqualifier le fournisseur préqualifié.

ébauche

c) Les répondants non retenus ne pourront pas participer aux étapes ultérieures du processus d'approvisionnement ni être évalués de nouveau à cette fin, à moins que le Canada décide, à sa seule discrétion, que les circonstances nécessitent une nouvelle évaluation.

d) Le Canada avisera par écrit chaque répondant de son statut de qualification.

4.4 Seconde vague de qualification de l'ISQ

a) Si le gouvernement du Canada fournit aux répondants non retenus une deuxième occasion de se qualifier, il leur fera tous parvenir par écrit, la même journée, les raisons pour lesquelles ils ne se sont pas qualifiés au cours de la première vague de qualification.

b) Si le gouvernement du Canada fournit aux répondants non retenus une deuxième occasion de se qualifier, il leur fera tous parvenir par écrit, la même journée, les raisons pour lesquelles ils ne se sont pas qualifiés au cours de la première vague de qualification.

c) Les répondants qui ne se qualifient pas à la suite de la seconde vague effectuée par le Canada ne pourront pas participer ou être évalués de nouveau pour les étapes ultérieures du processus d'approvisionnement.

ébauche

Annexe A: Preliminary Statement of Requirements

ébauche

Défense nationale National Defence

Sous-ministre adjoint (Gestion de l'information)

Énoncé préliminaire des besoins opérationnels (EBO)

Nº PSM	C.000707
TITRE	Cyberdéfense – Décision, analyse et réponse
ÉTAPE DU PROJET	Analyse des options
PROMOTEUR DU PROJET	Chef du personnel du cyberespace
ENTRÉE EN VIGUEUR	18 avril 2019
VERSION	1.6

Page laissée intentionnellement vide.

TABLE DES MATIÈRES

Liste des figures

Liste des tableaux

1. INTRODUCTION

1.1. Contexte [R7]

Le paysage des cybermenaces a fortement évolué depuis les deux dernières décennies. De nos jours, les cybercriminels usent de subterfuges beaucoup plus sophistiqués et et peuvent avoir à leur disposition d'importantes ressources; certains sont même financés par des États-nations ou le monde interlope. Leurs principales préoccupations consistent à acquérir les données de leurs adversaires et de miner leur capacité à mener des opérations dans le cyberespace. Les cybercriminels ont élaboré leurs méthodes de manière à contourner bon nombre de cyberdéfenses et se sont adaptés aux dispositifs informatiques mobiles ainsi qu'aux environnements infonuagiques afin d'exploiter les capacités de ces technologies. C'est pourquoi il est nécessaire d'adopter de nouvelles approches pour identifier rapidement les nouvelles menaces et accélérer la détection et les interventions, ce qui représente les capacités qu'offrira la solution CD-DAR.

À l'heure actuelle, les organisations déploient de nombreuses stratégies et technologies qui mettent l'accent sur une défense du réseau périmétrique ou des appareils des utilisateurs (ordinateurs portatifs, imprimantes, tablettes, etc.) fondée sur les méthodes d'attaque répertoriées (virus, maliciels, etc.). Ces solutions s'avèrent trop souvent inefficaces puisque susceptibles de produire une grande quantité d'alertes pour la plupart fausses. Impossibles à traiter automatiquement par un système, il faut donc analyser ces alertes à la main, ce qui nécessite beaucoup de temps et un important bassin d'experts. Parce que ces alertes sont très nombreuses, le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) ne disposent pas du temps nécessaire et de ressources pour intervenir chaque fois qu'une alerte est déclenchée, et doivent se résigner à ne pas les traiter toutes. Malgré les efforts déployés par le gouvernement, les attaquants font continuellement évoluer leurs méthodes pour contourner les cyberdéfenses et exploiter les changements technologiques, ce qui constitue une menace constante à la sécurité nationale et au bien-être du Canada et des Canadiens.

Le projet de CD-DAR, qui porte le numéro C.000707, servira à acquérir une solution de cyberdéfense (qui se traduit en capacités) dans le but d'améliorer l'aide à la décision en général et la sécurité du cyberespace du MDN et des FAC, y compris la capacité de détecter les menaces, de les analyser et d'y réagir. La solution intégrée fournira une analyse contextuelle fiable à l'appui des décisions et des mesures du MDN et des FAC à l'intérieur d'extensions et d'interfaces désignées du réseau de commandement[1] (R comd) ainsi que des systèmes du Réseau étendu de la Défense (RED) déployables à l'appui de la conduite d'opérations de cyberdéfense (OCD).

1.2. Énoncé des besoins opérationnels et résultats

1.2.1. Énoncé des besoins opérationnels [R7]

Le MDN et les FAC ont besoin d'une capacité de cyberdéfense applicable aux domaines stratégiques, opérationnels et propres à la mission. La capacité doit fournir une découverte du réseau, des outils de cyberdéfense logicielle intégrés, un dépôt de base de données de confiance et une image commune de la situation opérationnelle (ICSO), tenir compte des facteurs humains et permettre la criminalistique cybernétique à distance. Le MDN et les FAC ont besoin d'une capacité intégrée de surveillance de leur architecture de réseau et des renseignements qu'elle contient. Ils ont besoin de disposer d'une connaissance complète de la situation à partir de la détection et de l'analyse des cybermenaces, et d'élaborer une intervention en temps opportun et applicable à l'ensemble des domaines stratégiques, opérationnels et tactiques.

1.2.2. Facteurs de changement [R7]

[1] Le réseau de commandement est un réseau de communication qui relie un échelon de commandement à une partie ou à la totalité de ses échelons subalternes aux fins de commandement et de contrôle.

Il est actuellement difficile de découvrir et de suivre tous les actifs de réseau et de distinguer les éléments connus des éléments nouveaux (et inconnus). Des logiciels mal conçus et des composants du système mal configurés constituent des vulnérabilités importantes des systèmes d'information qui permettent leur exploitation. Afin de fournir des pratiques exemplaires en matière de sécurité des réseaux, telles qu'elles sont décrites par le Centre canadien pour la cybersécurité, le MDN et les FAC doivent commencer par comprendre la composition du réseau et disposer d'une solide capacité à en découvrir les actifs. Les analystes du Centre d'opérations des réseaux des Forces canadiennes (CORFC) travaillent souvent avec plusieurs trousses d'outils; ils doivent surveiller de nombreuses consoles pour être informés de nouvelles alertes, divers portails de services de renseignement sur les menaces pour obtenir de l'information sur les entités en cause et un éventail d'outils de détection et de réponse installés aux points d'extrémité pour comprendre ce qui se passe lorsque ces derniers sont touchés. Le CORFC utilise des outils de flux de travail pour contrôler les processus de triage et d'enquête; ce travail exige souvent que l'analyste copie et colle des données d'un outil à un autre, qu'il remplisse des formulaires et soumette des demandes de recherche ou qu'il téléverse des artéfacts aux fins d'analyse et d'entreposage. L'automatisation assurée par la solution CD-DAR élimine bon nombre de ces tâches, simplifie les processus et assure une qualité et une cohérence reproductibles, même si les processus demeurent essentiellement les mêmes. L'élimination partielle on complète de ce type de processus manuel répétitif aura une incidence directe sur la productivité des analystes de la sécurité. Ceux-ci pourront alors consacrer plus de temps à des problèmes plus épineux et davantage prioritaires qui exigent une expertise humaine.

De plus, on sait que les systèmes de surveillance de la sécurité génèrent un grand nombre d'alertes pour la plupart considérées comme des « faux résultats positifs » (ou tout simplement non pertinentes) après une enquête plus poussée. Le triage des alertes se fait souvent de façon manuelle par les analystes dont les erreurs toujours possibles se traduisent par l'omission d'incidents. De nombreux rapports dans les organismes de référence des médias sont tombés entre mauvaises mains même si les outils de sécurité ont généré une alerte à ce sujet, parce qu'un analyste l'a rejetée par erreur (probablement en raison d'une surcharge de travail). Le MDN et les FAC font face à des menaces de plus en plus agressives, comme des rançongiciels[2], où l'intervention efficace se mesure en secondes. Ce scénario oblige les organisations à réduire le temps qu'il leur faut pour réagir à ces incidents, habituellement en déléguant plus de tâches à des machines. La réduction du délai d'intervention, y compris le confinement des incidents et les mesures correctives, est l'un des moyens les plus efficaces de maîtriser les répercussions des incidents de sécurité. La solution CD-DARfournissent automatiquement un contexte aux alertes et ajoutent des renseignements clés pour permettre un triage manuel automatisé ou, à tout le moins, plus facile et plus rapide.

Le CORFC peut tirer parti d'une solution CD-DAR pour réduire le temps nécessaire à la formation des nouveaux analystes cybernétiques. L'automatisation élimine la nécessité pour l'analyste de connaître les détails des étapes manuelles à suivre pour chaque scénario. Les connaissances sont stockées et gérées dans la solution CD-DAR, ce qui réduira le besoin pour l'analyste de mémoriser le déroulement du processus et de le répéter constamment. Les analystes peuvent extraire des détails précis pour de nombreux scénarios, si le besoin se présente. Comme la solution CD-DAR combinera la fonctionnalité des outils existants et procurera une image commune de la situation opérationnelle, il ne sera plus autant nécessaire de donner de la formation à chaque analyste de la sécurité sur chacun des outils.

Le MDN et les FAC ne disposent pas d'une ICSO. L'exercice CWIX (Coalition Warrior Interoperability eXploration eXperiment eXamination eXercise) est un forum annuel portant sur le développement des capacités, la mise à l'essai de l'interopérabilité et l'expérimentation et organisé sous l'égide de l'OTAN. L'événement CWIX 2018 prévoyait effectuer des cas d'essai dans les domaines axés sur la cybernétique en mettant l'accent sur l'essai d'interopérabilité et l'expérimentation. Un des objectifs d'essai principal était d'examiner l'intégration des activités du domaine cybernétique dans une ICSO proposée, accompagnée des applications et des processus de

[2] Type de logiciel malveillant conçu pour bloquer l'accès à un système informatique jusqu'à ce qu'une somme d'argent soit payée.

commandement et de contrôle. Un total de 23 cas d'essai ont été établis, mais il a été impossible d'obtenir une ICSO. L'expérimentation a mené à la confirmation que des travaux supplémentaires sont nécessaires, et que la solution CD-DAR met davantage l'accent sur l'objectif de l'échelon supérieur d'une ICSO cybernétique.

On a conscience aujourd'hui que le nombre d'événements cybernétiques et d'alertes de sécurité surpasse facilement le nombre de cyberopérateurs ayant l'expérience et les qualifications nécessaires pour protéger et enquêter ces événements. Il est très difficile de demeurer à jour dans ce domaine en constante évolution. Qui plus est, les capacités de cyberdéfense inefficaces et désuètes font en sorte que la sécurité et la défense nationale au Canada demeurent vulnérables aux cybermenaces sans cesse grandissantes.

1.2.3. Lacunes en matière de capacités [R7]

Comme il est expliqué plus en détail à la section 1.3, les lacunes en matière de capacité sont des lacunes ou un manque de ce qui suit :

- découverte du réseau;
- outils de cyberdéfense logicielle intégrés;
- un dépôt de base de données fiable;
- image commune de la situation opérationnelle;
- facteurs humains;
- analyse judiciaire.

1.2.4. Résultats opérationnels [R7]

La solution CD-DAR apportera un changement fondamental à la cybersécurité du MDN et des FAC en mettant en œuvre la capacité d'intervention complète en cas d'événements de cybersécurité complexes et en évolution. Elle répondra aux besoins immédiats et à long terme, tout en maintenant et en permettant l'application des exigences en matière de cybersécurité.

Dans le cadre de ce projet, on livrera et mettra en œuvre un système complexe comprenant du matériel informatique et des logiciels, exploité par du personnel qualifié et suivant les processus connexes, qui assurera une surveillance fiable de la sécurité en temps quasi réel et exécutera une fonction d'intervention en cas d'événement sur les réseaux désignés.

Les résultats ***immédiats*** du projet feront du CORFC un centre moderne de cyberopérations doté d'une solution CD-DAR qui sera exploité par une cyberforce. La capacité qui sera mise en œuvre dans le cadre du projet aura une forte incidence sur la façon dont les cyberopérateurs sont sensibilisés, formés, équipés et mènent leurs activités quotidiennes. L'amélioration de l'aide à la décision et de l'analyse des décisions et réponse (ADR) permettra de s'assurer qu'ils sont prêts à fonctionner dans le cyberespace pour protéger les extensions et les interfaces du réseau de commandant du MDN et des FAC, ainsi que les systèmes du RED déployés.

Les résultats ***intermédiaires*** comprendront des indicateurs de rendement, des mesures de production de rapports et des systèmes de production de rapports (s'ils sont jugés essentiels), ainsi que des processus opérationnels perfectionnés et/ou nouvellement définis mis en place au besoin. Ces processus opérationnels utiliseront davantage le matériel et les outils logiciels pour établir une connaissance fiable, pertinente et significative de la situation de la cybersécurité de l'infrastructure des technologies de l'information (ITI), ainsi qu'une aide à la décision concernant les COD qui touchent tous les aspects des opérations du MDN et des FAC.

Les résultats ***ultimes*** de l'investissement proposé permettront au MDN et aux FAC d'avoir une cyberforce équipée, formée et prête à mener efficacement des activités de COD fondées sur une solide capacité cybernétique de base qui permettra de développer la croissance pour des années à venir. De plus, grâce à l'application de la politique de la Stratégie d'approvisionnement en matière de défense, ce projet contribuera au développement et au maintien d'une cyberindustrie viable au Canada qui est prête à soutenir le gouvernement du Canada et l'Équipe de

la Défense en offrant des technologies novatrices et avancées sur le plan scientifique ainsi qu'en dotation de personnel pour l'avenir.

1.2.5. Exigences obligatoires de haut niveau (EOHN)[R7]

Les principaux facteurs opérationnels de la capacité requise sont abordés par les exigences obligatoires de haut niveau. Les exigences obligatoires de haut niveau décrivent un ensemble de capacités que le projet de CD-DAR doit permettre d'atteindre. Essentiellement, ils définissent les résultats, les effets ou les services attendus du projet.

Les exigences obligatoires de haut niveau pour l'investissement sont décrites au Tableau 1 ci-dessous. Ces EOHN seront raffinés pour en faire un énoncé détaillé des besoins opérationnels (EBO).

Aux fins de l'EBO, la portée du projet de CD-DAR est le « réseau de commandement ». Un réseau de commandement est un réseau de communication qui relie un échelon de commandement à une partie ou à la totalité de ses échelons subalternes aux fins de commandement et de contrôle. L'infrastructure du réseau secret consolidé (IRSC) fait partie du réseau de commandement du MDN et des FAC et une partie importante de la portée de ce projet sera appliquée à l'IRSC. Le réseau de commandement comprend les extensions et les interfaces du R comd et les systèmes du RED déployables. Tout au long de cette analyse de rentabilisation, le terme « réseau de commandement » sera utilisé pour inclure les termes ci-dessus.

Tableau 1 – Exigences obligatoires de haut niveau

Nº	Capacité	EOHN
1	Cyberactifs (découverte du réseau)	La capacité d'identifier et de suivre rapidement tous les biens (autorisés et non autorisés) connectés au réseau de commandement et d'évaluer leurs attributs en matière de vulnérabilité, de configuration, de risque et de conformité aux correctifs.
2	Cyberanalyse	La capacité de recueillir, de conserver et d'analyser continuellement des renseignements sur les cybermenaces dans l'environnement du réseau de commandement et de détecter et de caractériser les activités suspectes, ainsi que de fournir un contexte pour les évaluations des risques et des vulnérabilités en temps quasi réel.
3	Intervention cybernétique	Capacité d'identifier de façon adaptative et dynamique une menace et de la contenir et de l'éradiquer.
4	Commandement et contrôle	La capacité de maintenir la connaissance de la situation, au moyen d'une image commune de la situation opérationnelle, des alertes, des menaces et des mesures correctives dans l'ensemble du réseau de commandement du MDN et des FAC, et d'alimenter la connaissance de la situation aux fins de prise de décisions et l'exécution des réponses par des interfaces normalisées et des flux de travail automatisés à l'appui du soutien à la décision de l'élément de commandement, et la mise en œuvre des interventions selon les directives.
5	Intégration de la solution CD-DAR	La capacité d'être intégrée (hébergée et exploitée avec des applications et un dépôt fiable) au réseau de commandement assigné en tant que système cohésif.

Nº	Capacité	EOHN
6	Cyberinteropérabilité	La capacité d'échanger des vecteurs de cybermenaces et d'analyser de l'information pour répondre aux exigences internes en matière de compatibilité ainsi qu'aux systèmes et à l'environnement réseau assigné d'autres ministères (AM) et des nations faisant partie du Groupe des cinq (Gp5), pays membres de l'Organisation du traité de l'Atlantique Nord (OTAN) et autres organisations externes.
7	Cyberrésilience	La capacité d'effectuer une surveillance localisée de l'architecture de réseau, des biens et de l'information sur les menaces, l'analyse et la prise de décisions d'intervention dans des environnements déployés où la connectivité n'est pas disponible, n'est pas fiable ou a une capacité limitée.
8	Évolution et développement continus des cybercapacités	La capacité d'évoluer continuellement en tant que réponse au changement (menace, politique, technologie) de l'infrastructure de réseau du MDN et des FAC (la criminalistique à distance et le confinement/l'assainissement font partie de cette intervention) avec une incidence minimale sur les systèmes connectés ou la modification de l'infrastructure de TI sous-jacente, des normes de base et des politiques.
9	Cyberflexibilité	La capacité de la solution CD-DAR à être évolutive, modulaire et facilement élargie, indépendamment de l'emplacement ou de la durée des actifs statiques ou opérationnels déployés.

1.2.6. Hypothèses clés [R7]

À la suite d'un examen interne et externe, les hypothèses touchant ce projet sont énumérées au Tableau 2 à la page suivante.

Tableau 2 – Hypothèses

Nº	Catégorie	Hypothèses utilisées	Effets sur le projet	Niveau de fiabilité faible/moyen/élevé	Stratégies si l'hypothèse ne se concrétise pas
1	Infrastructure	Le projet utilisera l'infrastructure physique et le réseau existant, mais pourrait nécessiter des réseaux enclavés particuliers à des fins de sécurité et d'essai.	Si l'infrastructure physique et le réseau existant ne peuvent pas être réutilisés, les coûts du projet augmenteront.	Élevé	Une réévaluation aura lieu et les fonds seront réaffectés.
2	Ingénierie des systèmes	La bande passante actuelle au sein de l'ITI permettra de tenir compte des mises à jour des données sur la connaissance de la situation (CS) que requieret la solution CD-DAR, particulièrement dans les emplacements déployés.	Un manque de bande passante disponible peut surcharger le cyberenvironnement opérationnel et nuire à l'assurance de la mission. Le besoin d'une bande passante supplémentaire augmenterait les coûts d'exploitation.	Élevé	S'il y a un manque de bande passante suffisante, il sera traité par les organismes appropriés (DIIGI, SPC) pour formuler une résolution

1.2.7. Capacité opérationnelle initiale (COI)

La COI verra l'atteinte de toutes les capacités de l'EOHN, comme l'illustre le tableau 1. Elle sera limitée aux infrastructures du réseau de commandement préétablies et aux actifs du RED déployés identifiés dans l'énoncé des besoins (EB) générés pendant la phase de définition du projet en consultation avec les intervenants et les experts en la matière (EM) concernés. Cela comprendra l'installation et la configuration de l'infrastructure de soutien aux sites concernés, où certains employés clés seront également formés sur les systèmes précis CD-DAR.

Cela permettra également d'atteindre des résultats opérationnels « immédiats » et « intermédiaires », comme il est indiqué dans les résultats opérationnels à la section 1.2.4 du présent document.

Avant la mise en œuvre, le promoteur du projet et l'exécutant s'entendront sur les exigences particulières en matière d'efficacité du système qui doivent être satisfaites pour indiquer l'obtention d'une COI. Le promoteur du projet et l'exécutant élaboreront conjointement un certificat de COI qui sera utilisé pour certifier la réalisation du jalon.

1.2.8. Capacité opérationnelle totale (COT)

La COT verra l'atteinte des capacités de tous les EOHN, décrites au tableau 1, sur le reste des infrastructures du réseau de commandement et des actifs du RED déployés. Les réseaux seront identifiés dans l'énoncé des besoins (EB) généré au cours de la phase de définition du projet et en consultation avec les intervenants et les experts en la matière (EM) concernés. Cela comprendra l'installation et la configuration de l'infrastructure de soutien et la formation de certains employés clés sur les systèmes de CD-DAR pour tous les sites concernés.

Outre les résultats opérationnels obtenus dans la COI sur les réseaux touchés, la COT atteindra également le résultat opérationnel « ultime », tel qu'il est mentionné à la section 1.2.4 Résultats opérationnels, offrant des capacités complètes de CD-DAR sur toutes les infrastructures du réseau de commandement et des actifs du RED déployés au sein des FAC.

Le promoteur du projet et l'exécutant s'entendront sur les exigences particulières en matière d'efficacité du système qui doivent être satisfaites pour indiquer l'obtention d'une COT. Le promoteur du projet et l'exécutant élaboreront conjointement un certificat de COT qui sera utilisé pour certifier la réalisation du jalon.

1.3. Insuffisance en capacités [R7]

Le domaine cybernétique du MDN et des FAC fait actuellement face à des menaces persistantes, constantes et croissantes de la part de ses adversaires. Il est essentiel que la solution CD-DAR remplace les systèmes multiples et les processus manuels d'aujourd'hui par une plate-forme unique et moderne, dotée de processus opérationnels corrélés et automatisés. Le projet de CD-DAR est un important pas en avant dans la défense et la protection du domaine cybernétique du MDN et des FAC avec un objectif centralisé sur le Groupe des opérations d'information des Forces canadiennes (GOIFC) et le Centre d'opérations des réseaux des Forces canadiennes (CORFC).

En collaboration avec des intervenants (c.-à-d. ceux ayant des intérêts particuliers dans le fonctionnement du réseau décrit ci-dessous, principalement au sein du MDN, ce qui comprend d'autres ministères ou organismes du gouvernement comme le CST et SPC, ainsi que le Groupe des cinq et les alliés de l'OTAN), le projet de CD-DAR a évalué les capacités cybernétiques du MDN et des FAC, et a conclu qu'elles sont insuffisantes pour les besoins actuels. Elles se fondent sur des solutions à court terme avec des injections irrégulières de nouvelles technologies qui permettent d'atteindre un effet limité. Au sein du MDN, le Centre d'opérations de réseaux des Forces canadiennes (CORFC) constitue l'organisation principale de cyberdéfense. Leur mission est d'obtenir et de maintenir la cybersupériorité au sein de la zone de responsabilité cybernétique (ZResp) du MDN et des FAC afin d'assurer la « liberté d'action des forces amies ». Concentrés sur les opérations, hautement motivés et possédant des compétences uniques en technologies et techniques spécialisées, ils sont proactifs, dynamiques, disponibles 24 heures sur 24, 7 jours sur 7 et se consacrent au maintien des services de TI dans toutes les conditions. Le CORFC est l'unité nationale opérationnelle de cyberdéfense qui se voit attribuer en permanence des tâches essentielles à la mission pour représenter le chef d'état-major de la Défense (CEMD) et les autorités opérationnelles de réseau (AO) applicables. Le CORFC dirige les opérations courantes et la défense de tous les réseaux du MDN et des FC pour le compte du SMA(GI).

Au sein du CORFC, les équipes suivantes présentent des lacunes en matière de capacité :

- Opération de cyberdéfense – coordonne les cyberopérations défensives du MDN et des FAC et l'intervention en cas d'incident avec les organisations internes et externes du Ministère;
- Cellule de renseignement sur les cybermenaces – fonctionne à l'heure actuelle de 8 à 17 h (avec une capacité de pointe) pour fournir des renseignements proactifs et réactifs afin d'améliorer les opérations de cyberdéfense;
- Équipe de surveillance – analyse du trafic réseau du domaine cybernétique du MDN et des FAC afin d'identifier les dispositifs potentiellement compromis en vue d'une enquête plus approfondie;

- Équipe de reconnaissance – fournit des évaluations réalistes et en direct de la vulnérabilité et de l'exploitation avancée des systèmes et des procédures d'information pour évaluer la posture de sécurité du client et effectuer des démonstrations contrôlées de ce qu'un attaquant pourrait accomplir dans l'infrastructure de TI d'un client;
- Équipe de gestion des incidents – assume le rôle de chef de file national en matière de gestion des incidents dans le cadre établi pour une approche d'entreprise coordonnée;
- Soutien du système de détection des intrusions d'entreprise – responsable de fournir un soutien 24 heures sur 24, 7 jours sur 7, des éléments suivants : (i) la configuration, la mise à l'essai, le déploiement de divers SDI et outils analytiques sur les capteurs/serveurs de SDI du CORFC pour tous les réseaux surveillés des FAC; (ii) la configuration, la mise à l'essai et le déploiement de divers capteurs/serveurs SDI sur tous les réseaux; (iii) les correctifs et les mises à niveau des suites de SDI nécessaires; et (iv) le soutien matériel et logiciel et la maintenance du matériel SDI (Security Onion[3], Sourcefire[4], conçus spécifiquement pour le CORFC);
- Équipe de soutien de l'évaluation des vulnérabilités de l'entreprise – s'occupe de la gestion des vulnérabilités et des risques dans certains réseaux;
- Section de la criminalistique – fournit des services d'analyse numérique spécialisés au MDN et aux FAC. Elle fournit également une analyse technique des cybermenaces et des techniques de logiciels malveillants utilisées par les adversaires pour pénétrer le domaine cybernétique du MDN et des FAC.

Les lacunes en matière de capacité sont des insuffisances ou un manque de ce qui suit :

- découverte du réseau;
- outils de cyberdéfense logicielle intégrés;
- un dépôt de base de données fiable;
- image commune de la situation opérationnelle;
- facteurs humains;
- analyse judiciaire.

Découverte du réseau – Afin de protéger un réseau, il doit y avoir un inventaire complet de tous les dispositifs matériels du réseau, comme les serveurs, les routeurs, les commutateurs, les passerelles et bien plus encore, et les logiciels, y compris les versions ou les correctifs[5] les plus récents qui se trouvent sur le réseau spécifié. À l'heure actuelle, la surveillance du réseau et la découverte d'appareils sont limitées pour le MDN et les FAC. Il y a des plates-formes capables d'effectuer la découverte de réseaux qui sont mises à l'essai et utilisées de façon ponctuelle, couvrant des parties des réseaux du MDN et des FAC, mais pas le réseau complet. Des logiciels comme Nessus, Cyber Information and Incident Sharing System (CIICS) et Malware Information Sharing Platform (MISP)[6] se sont révélés capables de fournir une solution, mais ne sont pas utilisés de façon cohérente. La

[3] Security Onion est une distribution Linux à source ouverte pour la détection des intrusions, la surveillance de la sécurité de l'entreprise et la gestion des journaux.

[4] Sourcefire, Inc. (acquis par Cisco) était une entreprise de technologie qui a mis au point du matériel et des logiciels de sécurité de réseau. Les dispositifs de sécurité de réseau Firepower de l'entreprise sont basés sur Snort, un système de détection d'intrusion (SDI) de source ouverte.

[5] Un correctif est un ensemble de modifications à un programme informatique ou ses données connexes pour les corriger ou les améliorer) Cela comprend la correction des vulnérabilités en matière de sécurité (une faiblesse qui peut être exploitée par un auteur de menaces, comme un attaquant, pour exécuter des actions non autorisées dans un système informatique).

[6] Nessus est un outil de balayage des vulnérabilités exclusif élaboré par Tenable Network Security; Cyber Information and Incident Coordination System (CIICS) est une application Web qui permet aux nations de partager des renseignements de cyberdéfense au sein d'une communauté fiable nommée NATO CIICS Federation. La plate-forme de partage des menaces, Malware Information Sharing

solution CD-DAR trouvera les meilleures réponses possibles, assurera l'interopérabilité des plates-formes de découverte de réseau et couvrira toute la gamme des capacités de conception de produits.

Outils de cyberdéfense logicielle intégrés – L'ensemble d'outils actuels n'est pas intégré et nécessite des compétences d'opérateur extrêmement spécialisées pour utiliser ces outils logiciels afin d'isoler tout problème, exporter de l'information et faire des comparaisons manuelles avec de l'information extraite d'autres outils logiciels. Voici deux exemples :

- Équipe de surveillance – À l'heure actuelle, l'analyste de la surveillance utilise des ensembles d'outils isolés qui ne sont pas reliés. Toutefois, cela ne nous donne pas un portrait complet du contexte des cybermenaces. Pour automatiser plus efficacement la détection des menaces, il faut utiliser l'apprentissage automatique et les algorithmes automatisés pour observer les tendances afin de détecter les menaces jusque-là inconnues. Cela aidera à maintenir la robustesse du réseau, ce qui permettra au MDN et aux FAC de maintenir une meilleure cybersécurité;
- Équipe de gestion des incidents – Le traitement des incidents est un processus très lourd. Il y a peu de plates-formes qui ont de bons flux de travail qui permettent la traçabilité de la façon dont un incident est traité et/ou qui assurent la responsabilisation des mesures prises tout au long du processus. À ce moment-là, une analyse est effectuée sur une plate-forme, puis les données d'analyse doivent être transférées physiquement à d'autres applications pour bien gérer l'incident.

Un dépôt de base de données fiable – La Cellule de renseignements sur les cybermenaces fournit des renseignements proactifs et réactifs pour améliorer les opérations de cyberdéfense. Pour effectuer une analyse, le MDN et les FAC doivent tirer des renseignements de différents systèmes. Un dépôt central permettra aux commandants de prendre des décisions éclairées sur les mesures défensives requises. À l'heure actuelle, le Centre national de transfert de données de l'état-major interarmées stratégique a la capacité de transférer de l'information à partir de 29 réseaux différents pour l'ensemble du MDN et des FAC. Toutefois, comme il ne s'agit pas d'une cybercapacité, cette information est hors de portée pour la solution CD-DAR et limite la façon dont l'information est stockée et transférée à des fins de cyberrenseignement. Il est nécessaire d'avoir des renseignements sur les cybermenaces adaptés à la tâche dans un dépôt central et robuste avec une grande quantité d'automatisation pour les sources fiables et connues, du niveau de classification faible au niveau de classification élevé (et vice versa), de l'information et des données de base du système et du réseau. Cela permettra la surveillance de la sécurité et des mécanismes comme l'analyse des liens, l'analyse des vulnérabilités, la détection des intrusions, l'analyse criminalistique, la collecte et l'analyse de journaux et d'autres données provenant des réseaux de l'organisation. Cela permettrait également d'effectuer des examens d'analyse de sécurité et de donner des conseils et des directives pour les interventions aux alertes de sécurité.

Image commune de la situation opérationnelle (ICSO) – La capacité de partager l'information nécessaire à l'élaboration d'une ICSO est étroitement associée aux outils de défense logicielle intégrée. Les capacités actuelles du MDN et des FAC ne disposent pas d'un point de vue central pour évaluer les répercussions des cyberactivités. Ces capacités sont insuffisamment intégrées, moins réactives et considérées comme déficientes pour ce qui est de fournir de l'information opérationnelle à l'appui des processus décisionnels efficaces du commandement. Une ICSO doit être souple et adaptée aux besoins de chaque commandant, qu'ils soient stratégiques, opérationnels ou tactiques. À l'heure actuelle, le CORFC utilise le programme interne et n'a aucune marge de manœuvre dans les points de vue opérationnels pour consolider l'information pour le commandant. Il est également impossible d'utiliser ce programme sur des réseaux qui ne sont pas disponibles, qui ne sont pas fiables ou qui ont une capacité limitée (épisodique).

Platform (MISP), est un logiciel gratuit et de source ouverte qui facilite l'échange d'information des renseignements sur les menaces, y compris les indicateurs de cybersécurité.

Facteurs humains – La solution CD-DAR abordera deux aspects particuliers des facteurs humains. Le premier est qu'il faut trop de spécialisation de la part des analystes cybernétiques, et le deuxième est la surcharge cognitive pour les cyberopérateurs. Pour régler ces problèmes, le projet de CD-DAR fournira une solution intégrée de cyberdéfense qui allégera le fardeau de comparer manuellement l'information d'un outil à celle d'un autre; cela réduira les connaissances détaillées et la spécialisation nécessaires pour maîtriser les divers outils de cyberdéfense. La solution CD-DAR atténuera la surcharge cognitive en gérant le volume de détection manuelle des menaces en recueillant automatiquement des renseignements de sécurité à partir du réseau. Elle analysera ces renseignements afin de cerner les menaces et de mettre en corrélation les renseignements provenant de sources multiples (gouvernement du Canada et alliés). Les alertes de sécurité seront alors automatiquement classées par ordre de priorité avec des recommandations sur la façon de remédier aux menaces.

La solution CD-DAR fera appel à des analyses de sécurité avancées qui vont bien au-delà des approches fondées sur la signature actuellement utilisées. Les technologies d'apprentissage automatique seront mises à profit pour évaluer les événements dans l'ensemble du réseau de commandement et détecter les menaces et prévoir l'évolution d'attaques qui seraient impossibles à réaliser au moyen d'approches manuelles. Ces analyses de sécurité comprennent :

- des renseignements intégrés sur les menaces qui ciblent les mauvais acteurs connus en tirant parti des renseignements sur les menaces mondiales;
- une analyse comportementale qui applique des modèles connus pour découvrir des comportements malveillants;
- la détection d'anomalies au moyen du profilage statistique pour établir une base de référence historique afin de fournir des alertes sur les écarts par rapport aux bases de référence établies qui sont conformes aux vecteurs d'attaque potentiels.

Capacité de mener des enquêtes judiciaires – La Section de la criminalistique fournit des services d'analyse numérique spécialisés au MDN et aux FAC. Elle fournit également une analyse technique des cybermenaces et des techniques de logiciels malveillants utilisées par les adversaires pour pénétrer le domaine cybernétique du MDN et des FAC. En plus de l'analyse des logiciels malveillants, la Section de la criminalistique est chargée de tenir à jour les événements de cybersécurité et de collaborer avec d'autres organismes. À l'heure actuelle, lorsqu'une fuite de données se produit, l'enlèvement physique et le remplacement du matériel peuvent coûter des milliers, voire des millions de dollars au MDN et aux FAC. Avec le projet CD-DAR comme solution de rechange au remplacement du matériel physique, l'image d'un disque dur touché pourrait être envoyée à distance à un environnement de bac à sable[7] où la Section de la criminalistique peut faire des analyses et des enquêtes tout en permettant d'effacer le disque dur. Lorsque l'équipement est situé dans différentes régions géographiques sans l'expertise d'un analyste, les disques durs et autres équipements doivent être expédiés à une installation locale aux fins d'analyse. Ces disques sont sujets à être endommagés au cours de l'expédition, ce qui entraîne des retards supplémentaires ou peut empêcher la mise en place d'une procédure appropriée et l'examen de preuves potentielles. La solution CD-DAR permettra d'économiser du temps et de l'argent, car la Section de la criminalistique n'aura pas à attendre que l'équipement soit transporté d'un bout à l'autre du pays à des fins d'analyse.

1.4. Contraintes liées au projet [R7]

[7] Dans le domaine de la sécurité informatique, un « bac à sable » est un mécanisme de sécurité qui permet de séparer les programmes en cours d'exécution, habituellement dans le but d'atténuer les défaillances du système ou les vulnérabilités du logiciel, sans risquer de nuire à la machine hôte ou au système d'exploitation.

Tableau 3 – Contraintes

Nº	Catégorie	Description
1	Exigences de conception	Le système de processus, de logiciels et de matériel doit pouvoir être utilisé par le personnel opérationnel existant du MDN et des FAC, y compris le personnel qui produit et utilise actuellement de l'information sur la connaissance de la situation.

1.5. Situation actuelle [R7]

Le 28 mars 2019, le Comité des capacités de la Défense (CCD)a passé en revue le projet de CD-DAR. Il a approuvé l'option préférée qui consiste à regrouper l'analyse de rentabilisation (projets de la SC et des AD-COD). Le CCD a également convenu que le projet devrait être acheminé au Conseil de gestion du programme pour qu'il appuie la phase de définition, à la suite de l'examen de la portée, de l'extensibilité et des calendriers du projet.

2. FONCTIONNEMENT DU SYSTÈME

2.1. Missions et scénarios

La **mission** de la cyberforce des FAC est d'imaginer et de concevoir les cybercapacités des FAC, puis de les construire et de les mettre en œuvre avec les forces existantes pour mener des cyberopérations complètes. Étant donné le domaine cybernétique constant, intégré, mondial et technologiquement dépendant dans lequel les FAC opèrent dans l'ensemble, la cyberforce joue un rôle crucial dans la défense quotidienne du Canada, maintenant et à l'avenir.

La **mission principale** du projet de CD-DAR consistera à acquérir des cybercapacités défensives pour améliorer la cybersécurité, la SC et l'analyse des décisions et réponse (ADR). Celles-ci doivent être intégrées dans une solution pour fournir une analyse contextuelle fiable afin d'appuyer les décisions et les mesures d'intervention du personnel du réseau de commandement dans la conduite des COD. [R3]

Le MDN et des FAC sont chargés du renseignement militaire à des fins d'évaluation de la menace et des risques. En tout temps, le MDN et des FAC peuvent être tenus d'entreprendre des missions pour assurer la protection du Canada et des Canadiens ainsi que le maintien de la paix et de la stabilité internationales.

Les capacités de CD-DAR seront disponibles et actives, peu importe le but, l'emplacement ou la durée de la mission. Étant donné que la solution CD-DAR surveille les R comd et leurs extensions, les opérations utilisant ces R comd bénéficieront de la même capacité de cyberdéfense à l'appui de leur mission.

Une cyberopération est l'application de cybercapacités coordonnées pour atteindre un objectif dans le cyberespace ou par son intermédiaire. [R24] Les cyberopérations sont pertinentes dans tout le spectre des opérations militaires, qu'il s'agisse du soutien à l'autorité civile, la recherche et le sauvetage, les opérations de soutien de la paix et de combat. [R25] Comme pour toutes les opérations militaires, les effets opérationnels sont produits par l'intermédiaire de relations de commandement et contrôle officialisées, de groupements opérationnels, de besoins en matière d'information déterminés par le commandement, d'une planification délibérée, de procédures d'état-major et d'une force entraînée et préparée capable de produire les effets opérationnels souhaités.

L'objectif des COD est de contrer activement les menaces et de restaurer l'état de fonctionnement sécuritaire initial du réseau. Les COD sont l'ensemble des mesures prises pour défendre la disponibilité, l'intégrité et la confidentialité du système de commandement et contrôle et des données des FAC de manière qu'un commandant puisse se prévaloir de ses pouvoirs opérationnels. Les actions associées aux COD comprennent les activités de soutien du renseignement (protection), les tâches de surveillance et de reconnaissance (détection et orientation), les décisions de commandement (décision) et le déploiement de contre-mesures (action).

Le diagramme de la Figure 1 de la page suivante présente un modèle d'action et de décision type pour les COD. IL montre également montre les relations et les plans servant à revenir à un état de fonctionnement sécuritaire.

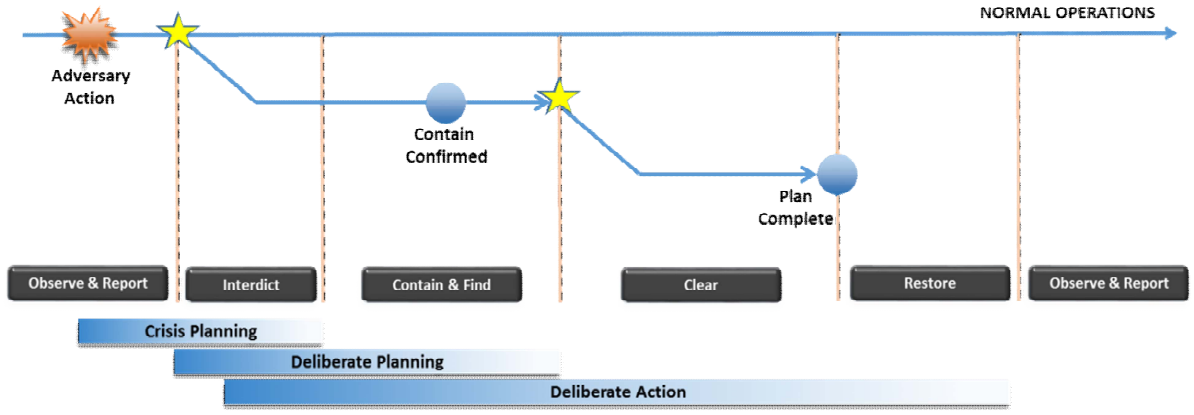


Figure 1 – Modèle d'action et de décision des COD

Une fois la solution CD-DAR mise en œuvre, le rôle du CORFC comprendra la détection, la reconnaissance et l'identification d'entités cybernétiques (humaines et non humaines) hostiles ou autrement non autorisées dans un secteur de responsabilité cybernétique défini et désigné et, selon sa disposition, préviendra sa destruction ou sa perte par les actions de l'ennemi.

Cybermission du CORFC : « La mission du CORFC consiste à obtenir et à maintenir la cybersupériorité à l'intérieur de la zone de responsabilité cyberspatiale du MDN et des FAC afin d'assurer la liberté d'action des forces amies. »

Le projet de CD-DAR fournira une capacité qui améliorera la position du MDN et des FAC en matière de cybersécurité, réduira le délai d'intervention en cas d'incidents cybernétiques et aidera à atténuer la menace d'attaque cybernétique en fournissant à l'utilisateur d'une force un moyen de fonctionner efficacement dans un domaine cybernétique contesté. La visibilité accrue en matière de sécurité et la normalisation assurée par la solution CD-DAR constitueront le fondement sur lequel des capacités plus avancées de gestion, de sécurité et de défense du Canada et des Canadiens pourront être construites.

2.2. Environnement

Étant donné qu'une partie importante de la population mondiale est maintenant connectée à l'échelle mondiale grâce à l'évolution d'Internet, les défis que pose le cyberespace en matière de sécurité et de défense sont importants. En outre, une connectivité accrue a permis et continuera de permettre aux adversaires de se connecter à des groupes idéologiques et à des individus et de les motiver grâce à une gamme de plates-formes Internet, de devises et de sources de pouvoir financier. La protection du renseignement, de la défense et de l'information sur la sécurité nationale, l'accès garanti et l'utilisation des systèmes et de l'infrastructure des technologies de l'information du Canada et des pays alliés; et la capacité d'exploiter le cyberespace pour atteindre les objectifs de sécurité nationale est une nécessité et continuera d'être essentielle à la sécurité de la plupart des pays. [R7]

L'importance de l'ITI mondiale continue de s'étendre à de nouveaux domaines de la vie moderne et de la société. Les avancées technologiques ont ouvert le domaine cybernétique à une variété d'acteurs étatiques et non étatiques; ce qui donne lieu à l'augmentation de menaces importantes. Dans le contexte militaire, les adversaires potentiels développent rapidement des moyens cybernétiques pour exploiter les vulnérabilités inhérentes aux systèmes de commandement, de contrôle, de communications, de l'informatique, de renseignement, de surveillance et de reconnaissance (C4ISR) ainsi que les systèmes de combat. Cette exigence militaire et intérieure principale est décrite dans la politique de défense du Canada : Protection, Sécurité, Engagement [R6]

La solution CD-DAR fournira des capacités de sécurité et de défense des TI partout où les extensions et interfaces du R comd, statiques et déployables, et les systèmes de RED déployables identifiés sont accessibles. Cela a une incidence sur les environnements suivants :

a. *Environnement durable*. Cela comprend les emplacements fixes au pays et à l'étranger, comme le Centre des opérations du réseau des Forces canadiennes (CORFC) et le COSD lorsqu'il y a une gamme complète d'infrastructures de soutien disponibles ainsi qu'une connectivité complète aux réseaux et systèmes de soutien. L'environnement opérationnel est robuste et fiable;

b. *Environnement épisodique*. Cela concerne tous les lieux de mission où l'infrastructure variera de robuste à limitée, et la disponibilité variera de fiable à non fiable. Ces conditions s'ajoutent aux exigences de fonctionnement dans des situations débranchées, intermittentes et à faible largeur de bande (limitée) et de reprise après une telle situation. Les environnements débranchés, intermittents et limités présupposent le besoin de traitement autonome local, de voies de communication de rechange et de la capacité de se rétablir sans problème des limites de connexion lorsque la connexion est rétablie;

c. *Environnement de collaboration*. Comme la plupart des missions du MDN et des FAC sont menées dans des environnements de systèmes et parties multiples, les capacités de CD-DAR doivent être interopérables avec les réseaux et systèmes gérés par le MDN, les autres ministères et organismes, les alliés et d'autres partenaires internationaux. La solution CD-DAR doit également tenir compte de la nécessité de traiter l'information dans divers domaines de sécurité et mises en garde.

d. *Cyberenvironnement*. Les faiblesses peuvent être exploitées et les répercussions de ces exploitations peuvent être réparties entre les réseaux qui exigent une réactivité maximale. Pour ce faire, on optimise habituellement l'automatisation des capacités de surveillance, de détection, d'analyse, de prise de décisions et d'intervention, ainsi que l'inclusion de processus et de systèmes souples pour s'adapter à un environnement de menace en évolution rapide.

Le domaine cybernétique nécessite un ensemble solide et cohérent d'outils, de ressources et de capacités pour permettre au MDN et aux FAC de remplir leur mandat et de fonctionner efficacement dans un domaine cybernétique contesté.

2.3. Menaces

Tout comme la guerre asymétrique, les cybermenaces[8] ne sont pas immédiatement visibles par rapport aux conflits militaires traditionnels. D'innombrables acteurs menaçants, cachés dans le cyberespace, peuvent influencer ou cibler le MDN ou les FAC dans leur ensemble, un système précis ou une personne en particulier.

Pour concentrer les efforts de défense dans le cyberdomaine, le Canada doit avoir une bonne connaissance des auteurs des menaces, y compris de leurs intentions, leurs capacités et leurs occasions. Un rapport en libre accès produit par les États-Unis, *The Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee* [R38], identifie certains des principaux auteurs de cybermenaces et les menaces qu'ils posent. Les points suivants tirés du rapport sont mis en évidence pour illustrer l'utilisation du cyberespace par nos adversaires dans l'environnement opérationnel :

a. Certaines nations adoptent une posture cyberspatiale plus ferme en fonction de leur volonté de cibler les systèmes d'infrastructure essentiels et de mener des opérations d'espionnage même lorsqu'elles sont détectées et sous un contrôle public accru.

[8] Cybermenace (OTAN) : La possibilité de tentative malveillante visant à endommager ou perturber un système ou un réseau informatique.

b. Les cyberopérations sont susceptibles de cibler les intérêts de l'Occident pour soutenir plusieurs objectifs stratégiques : la collecte de renseignements[9] pour soutenir la prise de décision, influencer les opérations pour soutenir les objectifs militaires et politiques et poursuivre la préparation du cyberenvironnement pour les événements imprévus futurs.

c. Plusieurs pays continuent d'avoir du succès dans le cyberespionnage contre les gouvernements et l'industrie.

d. Les cyberattaques sont utilisées contre des cibles qui représentent une menace à la stabilité nationale ou à la légitimité du régime.

e. L'espionnage, la propagande et les attaques dans le cyberespace sont utilisés pour soutenir les priorités en matière de sécurité, influencer les événements et contrecarrer les menaces.

f. Certaines nations sont capables de lancer des cyberattaques perturbatrices ou destructrices pour soutenir des objectifs politiques et elles sont disposées à le faire.[R4]

Les cybermenaces les plus évoluées proviennent des services de renseignements et des services militaires d'états étrangers. Les gouvernements avancés sur le plan technologique, leurs forces militaires et les entreprises privées sont vulnérables au cyberespionnage parrainé par des États et aux cyberopérations perturbatrices. On peut s'attendre à ce que cette menace augmente au cours des prochaines années.

Les cyberopérations ennemies créent des menaces importantes pour les missions alliées menées dans le cyberespace ou au moyen de celui-ci, où les ennemis peuvent interdire l'accès aux capacités opérationnelles où les manipuler; mener des collectes de renseignements rapides et régulières; et mener des activités de déception. L'enjeu opérationnel est donc de s'assurer de la liberté d'action des FAC dans le cyberespace en défendant les capacités des FAC en appui aux objectifs militaires.[R4]

Dans un contexte militaire, alors que l'utilisation du cyberespace est devenue essentielle aux opérations, les adversaires potentiels, y compris les intermédiaires étatiques et les acteurs non étatiques, développent rapidement des moyens cybernétiques d'exploiter les vulnérabilités inhérentes aux systèmes de C4ISR sur lesquels l'armée dépend, ainsi que les technologies opérationnelles comme les systèmes de combat.[R7]

Le taux élevé d'innovation technologique, la domination des logiciels commerciaux et la prolifération croissante d'entités dotées de logiciels intégrés et immuables signifient que le potentiel de cyberattaque dépassera les capacités de défense.[R26]

a. L'utilisation continue de technologie commerciale signifie que les vulnérabilités des systèmes peuvent être connues, échangées et grandement exploitées. L'interdépendance fondée sur des réseaux reliés rend d'importants systèmes très vulnérables à un effondrement rapide et catastrophique, ce qui nécessite une étape de réparation prolongée. À mesure que le nombre de cybertransactions augmente, la proportion relative d'attaques peut diminuer. Toutefois, le risque d'attaques catastrophiques ne cesse d'augmenter.

b. La prolifération d'appareils avec des systèmes intégrés — l'Internet des objets — ajoute un nouveau danger. Les appareils seront durables, vulnérables aux attaques, et il sera impossible de corriger leur logiciel.

[9] Renseignement : Produit de la recherche, du traitement, de l'analyse, de l'intégration et de l'interprétation des informations disponibles sur les États étrangers, les forces ou éléments hostiles ou susceptibles de l'être, la géographie et les facteurs sociaux et culturels qui contribuent à la compréhension de l'environnement opérationnel réel ou potentiel.

Remarque : Le terme « renseignement » décrit également les activités qui mènent au produit, ainsi que les organisations qui les exécutent. BTD, fiche 738.

c. L'utilisation par l'État d'armes de cyberattaque ne sera pas limitée principalement en raison de son efficacité et de l'anonymat que procure le cyberespace, ce qui rend certaines attaques pratiquement impossibles à retracer.

2.4. Concept des opérations

Compte tenu de la complexité des environnements opérationnels modernes, il existe un besoin continu d'une connaissance de la situation, d'un partage de l'information et d'une collaboration en temps réel, satisfait au moyen d'une capacité de gestion de l'espace de bataille cybernétique, plus connue sous le nom d'image commune de la situation opérationnelle (ICSO). Une capacité de gestion de l'espace de bataille cybernétique doit offrir la capacité de fusionner, de corréler et d'afficher des données de capteurs de réseaux mondiaux rapidement pour obtenir une vue d'ensemble fiable des réseaux amis, neutres et adversaires, notamment leur emplacement physique et leurs activités. De plus, une capacité de gestion de l'espace de bataille cybernétique vise à appuyer les données au sujet de la menace ou de l'événement en temps quasi réel d'une myriade de sources et à améliorer la capacité des commandants à identifier, à surveiller, à caractériser et à repérer une activité du domaine cybernétique qui a lieu à la fois au niveau mondial et dans les zones de responsabilité (ZResp), et à intervenir en réaction à cette action.

> « L'efficacité globale des cyberopérations est déterminée par la capacité d'intégrer rapidement la connaissance de la situation, la compréhension et les interventions dans les opérations des réseaux et les activités des cyberopérations. Cela sous-entend un besoin de centraliser les unités et un désir de réduire le quartier général qui exerce le C2 au minimum. Du point de vue de la défense, cela est particulièrement important en ce qui a trait au développement de la connaissance de la situation du cyberespace, qui est importante pour les opérations de réseaux, mais qui représente le centre de gravité pour les COD. Le C2 devrait être aussi horizontal que possible et optimisé pour être réactif en fonction des autorités pertinentes déléguées pour intervenir rapidement[10]. Du point de vue de la structure de la force, cela crée des unités de COD intégrées, à la fois responsables du développement et du maintien de la connaissance de la situation du cyberdomaine vaste et autorisées à mener des interventions rapides et directes avec des éléments dispersés des opérations de réseaux. [R4]

Les forces menant les cyberopérations peuvent avoir à soutenir simultanément plusieurs utilisateurs. Cela nécessite une coordination étendue, une planification et une intégration précoce des exigences et des capacités. Les commandants appuyés et les commandants en appui coordonnent de manière appropriée le déploiement et l'emploi des forces menant les cyberopérations nécessaires à l'accomplissement de la mission attribuée, particulièrement pour les systèmes d'armes et de plates-formes déployés. La plupart des cyberopérations sont géographiquement séparées par un théâtre d'opérations appuyé; ainsi, tous les commandants concernés doivent prendre des mesures supplémentaires pour s'assurer que le commandant appuyé est continuellement informé de l'état opérationnel des forces en appui.

Avec la solution CD-DAR, les opérateurs cybernétiques sont le personnel chargé de la cybersécurité et des COD. Ces opérateurs sont en première ligne des opérations des FAC, en soutenant le commandant de la composante cybernétique des forces interarmées (CCCFI) dans ses tâches. En établissant la capacité, les autorisations organisationnelles, les politiques habilitantes et les processus opérationnels sont mis en place pour permettre à la capacité des opérations de cybersécurité défensives d'exécuter sa mission. La Figure 2 fournit une vue opérationnelle de haut niveau du système souhaité où les cyberopérateurs sont le personnel chargé de la cybersécurité et des COD.

[10] Il s'agit d'un extrait des cyberopérations de NDI; la structure de C2 étant « aussi plate que possible » signifie que le pouvoir de commandement devrait être délégué le plus près possible de l'exécution de l'intervention tactique, ce qui permet la réactivité des segments de l'intervention directe de la boucle OODA.

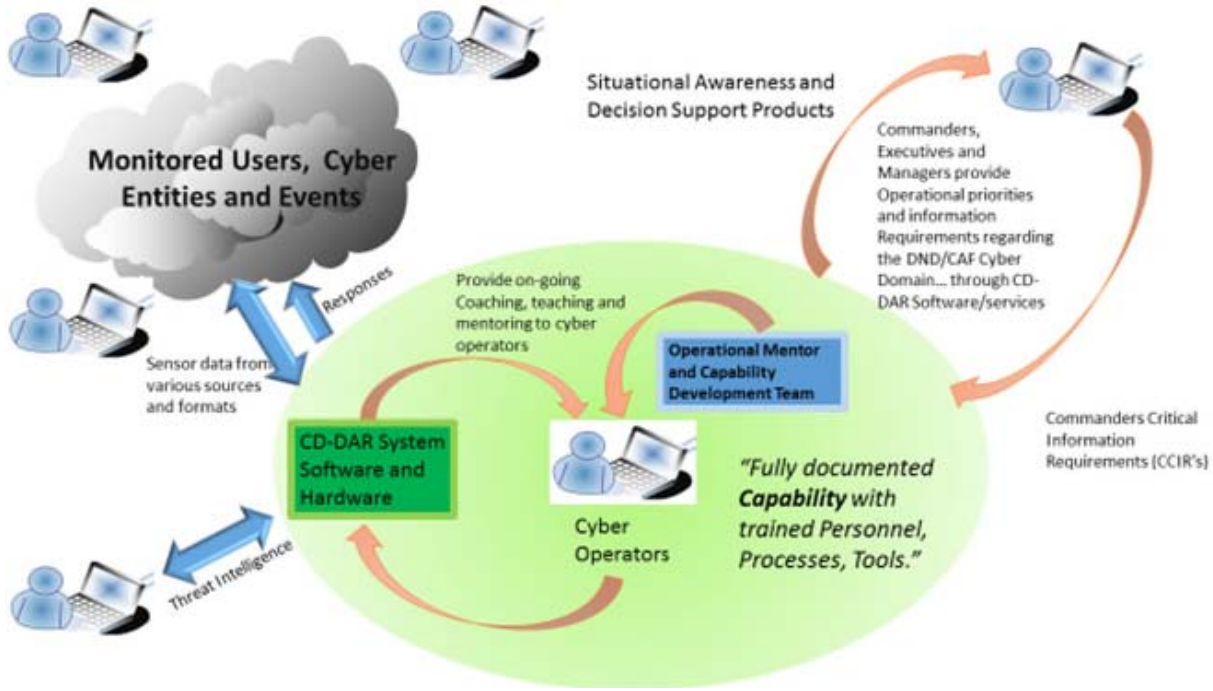


Figure 2 – Vue opérationnelle : centre des cyberopérations

Le projet de CD-DAR permettra de créer, d'équiper, d'organiser et de former le CORFC afin qu'il puisse exploiter une capacité qui défend les réseaux du MDN et des FAC dans l'environnement actuel, 24 heures sur 24, 7 jours sur 7, tout en offrant une instruction initiale, une instruction continue, du perfectionnement professionnel et le mentorat des cyberopérateurs du MDN et des FAC qui peuvent être déployés pour appuyer les opérations de cybersécurité et de défense du MDN et des FAC au pays ou à l'étranger.

La vue actuelle voit tous les cyberopérateurs et les autres utilisateurs (gestionnaires, cadres supérieurs, commandants et leurs états-majors) accomplir leurs tâches dans un seul environnement intégré. Ces tâches comprennent, sans toutefois s'y limiter : le flux de travail, le suivi, l'analyse, l'alerte, la production de rapports, la connaissance de la situation, les interventions et l'instruction (individuelle et collective). Chaque cyberopérateur a accès à un outil de visualisation du tableau de bord commun, adapté à son rôle et à ses responsabilités particulières. Les membres du personnel comme les cadres supérieurs, les commandants, les gestionnaires et d'autres éléments des opérations du réseau du MDN et des FAC (comme la Marine royale canadienne [MRC], l'Aviation royale canadienne [ARC], l'Armée canadienne [AC]), le Commandement des opérations interarmées du Canada (COIC), le Commandement des Forces d'opérations spéciales du Canada (COMFOSCAN) et l'État-major interarmées stratégique (EMIS) seraient également autorisés à fournir le niveau d'information approprié à des fins opérationnelles.

2.5. Concept de soutien [R39]

Ce concept de soutien indiquera comment le soutien en service (SES) et l'évolution de la capacité de CD-DAR, en tant que système opérationnel, seront effectués du point de vue technique et opérationnel.

2.5.1. Concept de soutien technique

Le SES technique pour la solution CD-DAR désigne le soutien en service de installations de TI et les actifs de TI touchés par cette technologie.

Pour la solution CD-DAR, cette catégorie comprend :

a. les salles de serveurs où l'information sur la sécurité des actifs est recueillie, agrégée, analysée, signalée et traitée;

b. l'Environnement d'essai cyberintégré (EECI).

Le SES des installations de TI est hors du champ d'application, car on suppose que les processus existants des installations de TI seront utilisés.

Le SES des actifs de TI comprend le soutien des systèmes d'information, des logiciels et du matériel entrant dans le cadre du projet et de l'information qu'ils traitent.

Pour la solution CD-DAR, les actifs de TI :

a. *incluent* les systèmes d'information, le matériel, les logiciels et les renseignements connexes dont dépend la solution CD-DAR (p. ex., pour la surveillance, la détection, l'analyse, la prise de décisions et les interventions liées à la sécurité et à la défense);

b. *excluent* tout système d'information, le matériel et les logiciels sur lesquels la fonctionnalité CD-DAR agit (p. ex., les appareils qu'elle surveille).

Le sous-ministre adjoint (Gestion de l'information) (SMA[GI]) sera chargé de soutenir les installations et les actifs, en tirant parti de l'organisation mise en œuvre dans le cadre du projet de la Gestion des services de technologie de l'information (GSTI) ou de sous-traiter les services, selon le cas.

Le soutien au système suivra le cadre de la Bibliothèque de l'infrastructure des technologies de l'information (BITI), qui appuie l'harmonisation des services de TI avec les besoins de l'entreprise. La BITI représente les pratiques exemplaires de l'industrie en matière de soutien des systèmes de TI. Ces pratiques exemplaires seront adaptées à l'environnement et la structure organisationnelle uniques du MDN et des FAC.

Trois lignes de soutien sont définies dans la BITI :

a. Soutien de première ligne. Le soutien de première ligne, qui porte sur la consignation et le classement des incidents reçus et sur l'intervention immédiate menée dans le but de tenter de rétablir dès que possible un service tombé en panne. Si une solution immédiate ne peut être obtenue, le soutien de premier niveau transmettra le problème au soutien de deuxième niveau. Le soutien de premier niveau traite aussi les demandes de service et tient les utilisateurs au courant de l'état de résolution des problèmes.

b. Soutien de deuxième ligne. Le soutien de deuxième ligne se charge des incidents qui ne peuvent pas être résolus immédiatement par le soutien de première ligne. Le soutien de deuxième ligne assurera la coordination avec les fournisseurs de services externes, suivant les besoins. Les problèmes qui ne peuvent pas être résolus à ce niveau sont transmis au soutien de troisième ligne.

c. Soutien de troisième ligne (national). Le soutien de troisième ligne est assuré par des fabricants de matériel et de logiciels ou des fournisseurs tiers. Les services sont demandés par le soutien de deuxième ligne pour résoudre un incident.

Le tableau ci-dessous décrit les lignes de soutien au sein du MDN avec les délais d'intervention et de réparation.

Tableau 4 – Temps de soutien du MDN

Niveau de l'installation de soutien	Délais d'intervention	Délais de réparation
Soutien de première ligne	Immédiatement (service de dépannage) Moins d'une heure	Effort continu
Soutien de deuxième ligne	À confirmer	À confirmer
Soutien de troisième ligne	À confirmer (selon le contrat ou l'entente sur les niveaux de service)	À confirmer

Le CONSUP détaillé sera élaboré pendant la phase de définition du projet, alors que la conception du système, les mesures de rendement principales et les spécifications fonctionnelles seront définies.

2.5.2. Concept d'affaires du soutien

Une capacité de mentorat opérationnel et de développement de capacité (MODC) est une petite équipe composée de spécialistes des cyberopérations militaires, de la fonction publique et des services professionnels; qui sera située au même endroit que la capacité livrée pendant la mise en œuvre et tout au long de son cycle de vie. Le rôle des équipes de MODC est d'entraîner, de former et de guider les cyberopérateurs (de tous les grades) pour qu'ils réalisent leur mission grâce à la transformation opérationnelle continue, au développement des compétences, au développement et à la coordination de l'instruction collective, et au développement et au soutien des outils cybernétiques. En collaboration avec les organisations touchées par la solution CD-DAR, le MODC est responsable de :

a. soutenir la transformation opérationnelle des capacités de cybersécurité et des COD des FAC afin qu'elles deviennent des capacités d'opérations de sécurité du NIST (National Institute of Standards and Technology);
b. soutenir les opérations de cybersécurité et les COD;
c. guider les cyberopérateurs à tous les niveaux pour améliorer leurs compétences et améliorer les cyberopérations des FAC afin d'assurer le maintien des compétences.

Le secteur de responsabilité type comprend :

a. Processus et organisations (planification et gestion, recherche et développement, concept et doctrine, conception organisationnelle, processus opérationnels, administration des affaires, services juridiques, services de sécurité);
b. Gestion des ressources humaines (gestion du personnel civil, gestion du personnel militaire, gestion des entrepreneurs, instruction);
c. Gestion des ressources matérielles (installations, équipement d'infrastructure matérielle, fournitures et approvisionnement);
d. Gestion des ressources financières (financement du personnel, du fonctionnement et de l'entretien [PF&E]).

Pour la solution CD-DAR, cela comprend :

a. les organisations qui régissent les opérations de CD-DAR, comme le commandant de la cyberforce;
b. les organisations participant à l'utilisation des capacités de CD-DAR, comme l'équipe interarmées des cyperopérations (EICO), le COSD et le CORFC.

2.6. Rôles clés [R30]

a. Commandants des FAC. Les commandants des FAC, jusqu'au CEMD inclusivement, sont responsables du C2 des forces affectées, y compris la cyberforce.

b. Personnel de soutien aux opérations. Le personnel de soutien opérationnel comprend toutes les personnes du MDN et des FAC qui fournissent un soutien direct et indirect aux activités de planification et d'exécution de la mission du commandant stratégique et opérationnel des FAC. Ils sont souvent situés au quartier général.

c. Personnel fournisseur de services. Le personnel qui met en œuvre et la solution CD-DAR et qui la met à la disposition des utilisateurs. Le CORFC est inclus pour le soutien opérationnel ainsi que pour le traitement des incidents et des événements de sécurité. Le rôle d'opérateur cybernétique est également inclus.

d. Autorité opérationnelle (AO). L'AO est définie comme la personne qui a le pouvoir de définir les exigences et les principes opérationnels, d'établir des normes et d'accepter le risque dans son secteur de responsabilité; l'AO est responsable envers le Chef d'état-major de la Défense[3]. En supposant qu'il n'y aura pas de changements importants à l'organisation et à la gouvernance de la TI dans un avenir prévisible, le DOS de l'EMIS sera l'AO pour l'infrastructure dans le cadre de la solution CD-DAR.

e. Responsable technique (RT). Le RT est désigné comme la personne qui possède l'autorité d'établir des normes et des exigences techniques, de gérer les configurations, de formuler des conseils techniques et de surveiller le respect des éléments dans son domaine de responsabilité. En supposant qu'il n'y aura pas de changements importants à l'organisation et à la gouvernance de la TI dans un avenir prévisible, le SMA(GI) sera le RT pour l'infrastructure dans le cadre de la solution CD-DAR.

f. Responsable de la sécurité. Le responsable de la sécurité est désigné comme la personne qui a l'autorité de relever les risques, de fournir des conseils et des normes de sécurité en vue de leur approbation par les responsables opérationnels et techniques, et de veiller à la conformité à ces normes dans son domaine de responsabilité. En supposant qu'il n'y aura pas de changements importants à l'organisation et à la gouvernance de la TI dans un avenir prévisible, le SMA(GI)/Directeur – Sécurité (Gestion de l'information) (Dir Sécur GI) sera le responsable de la sécurité pour l'infrastructure dans le cadre de la solution CD-DAR.

g. Autorité d'instruction. L'autorité d'instruction est désignée comme le commandant d'instruction ou d'un commandement qui est responsable d'un groupe professionnel militaire ou d'une branche et qui commande un centre de soutien de l'apprentissage et un ou plusieurs établissements d'instruction ou centres d'expertise fonctionnels. En supposant qu'il n'y aura pas de changements organisationnels importants dans un avenir prévisible, l'École d'électronique et des communications des Forces canadiennes (EECFC) sera l'autorité d'instruction pour les capacités offertes dans le cadre de ce projet.

h. Mentorat et développement des capacités. Cela consiste à guider les cyberopérateurs à tous les niveaux pour améliorer leurs compétences et améliorer les cyberopérations des FAC afin d'assurer le maintien des compétences. Plus concrètement, le rôle du mentor est d'entraîner, de former et de guider les cyberopérateurs pour qu'ils réalisent leur mission grâce à la transformation opérationnelle continue, au développement des compétences, au développement et à la coordination de l'instruction collective, et au développement et au soutien des outils cybernétiques.

2.7. Principales tâches

Tous les cyberopérateurs et les autres utilisateurs (gestionnaires, cadres supérieurs, commandants et leurs états-majors) accomplissent leurs tâches dans un seul environnement intégré. Ces tâches comprennent : le flux de travail, le suivi, l'analyse, l'alerte, la production de rapports, la connaissance de la situation, les interventions et l'instruction (individuelle et collective). Chaque cyberopérateur a accès à un outil de visualisation du tableau de bord commun, adapté à son rôle et à ses responsabilités particulières.

La CS du domaine cybernétique est regroupée au niveau du CORFC (par l'entremise de la solution CD-DAR) et transmise au personnel clé, comme les cadres supérieurs, les commandants, les gestionnaires et d'autres éléments

opérationnels du réseau du MDN et des FAC, comme la MRC, l'ARC, l'AC, le COIC, le COMFOSCAN et l'EMIS.

La solution CD-DAR appuie un certain nombre de tâches et de fonctions liées aux cyberopérations qui ont été définies dans la Note de doctrine interarmées[R4] sur les cyberopérations pour appuyer les opérations de réseau, les cyberopérations de soutien, la cybersécurité et les scénarios de cyberdéfense. Les tâches et les fonctions des COD seront analysées plus à fond ultérieurement.

2.8. Caractéristiques des utilisateurs

Comme il est indiqué à la section 2.1, la solution CD-DAR fournira une vue en temps quasi réel du réseau de commandement et de l'état de sécurité du réseau assigné. La solution CD-DAR contribuera également à faire en sorte que les systèmes ne subissent pas de répercussions négatives en surveillant continuellement les réseaux du MDN et des FAC avec l'aide des cyberopérateurs. Les cyberopérateurs sont le personnel chargé de la cybersécurité et des COD.

2.8.1. Cyberopérateurs

Les cyberopérateurs sont l'épine dorsale de la cyberforce. Il s'agit du personnel, à tous les niveaux hiérarchiques, dont le rôle principal est de : « détecter, reconnaître et identifier les cyberentités hostiles ou autrement non autorisées et contribuer à la destruction, à la neutralisation, à la suppression ou à l'élimination de l'ennemi dans le cyberespace et par d'autres moyens ».

Les cyberopérateurs dirigent les COD, assurent la liaison et travaillent en collaboration avec d'autres ministères et organismes, ainsi qu'avec les alliés du Canada, afin d'améliorer la capacité du MDN et des FAC de fournir un cyberenvironnement sécurisé. Ils surveillent les réseaux de communication des FAC afin de déceler toute tentative d'accès non autorisé et d'intervenir face à celles-ci. Ils fourniront aussi un cyberappui afin de combler les besoins opérationnels des FAC Compétences des cyberopérateurs.

Il ne faut pas confondre le métier de cyberopérateur avec celui de technicien des systèmes d'information et de télécommunications aérospatiales (SITA), de spécialiste des systèmes de communication et d'information de l'Armée de terre (SSCIAT), d'opérateurs d'équipement d'information de combat (Marine) (OP EICM), et les métiers des communicateurs navals (COMM N). Ces groupes professionnels militaires s'occupent principalement de la configuration, l'installation, l'exploitation et la maintenance des réseaux de communication et de l'ITI, tandis que les cyberopérateurs se concentrent sur la surveillance et la protection de l'ITI contre les menaces hostiles et le refus de l'utilisation du cyberespace par les forces hostiles. Les 26 emplois pour les cyberopérateurs (CYBEROP, 00378) peuvent être exécutés par le personnel de la force régulière ou de la réserve, sauf pour le poste le plus élevé dans le groupe professionnel, c'est-à-dire celui de conseiller cybernétique.

Les cyberopérateurs sont formés et éduqués à l'art de la cyberguerre en portant une attention particulière aux aspects suivants :

a. la nature du cyberespace et du domaine cybernétique;
b. les menaces, les acteurs de la menace et leur impact sur le cyberespace;
c. les principes et techniques de détection, de reconnaissance, d'identification et d'attribution de toutes les natures des entités cybernétiques;
d. les principes et techniques des COD, y compris les mesures de défense internes (MDI) et les mesures d'intervention (MI);
e. les tactiques, techniques et procédures pour :
    i la coordination du soutien cybernétique;
    ii le commandement et le contrôle;

iii la cyberreconnaissance;
iv la cybersurveillance;
v la gestion des cyberincidents;
vi la criminalistique cybernétique;
vii l'identification des cybermenaces;
viii les fonctions du Centre des cyberopérations.

3. DIRECTIVES RELATIVES AU PLAN ET À LA CONCEPTION

La solution CD-DAR permettra au MDN et aux FAC de mener des opérations de cybersécurité et donnera au CORFC/COSD la capacité de fournir des CS cybernétiques, de défendre les environnements de réseau du MDN et des FAC et de mener des COD. À cette fin, la capacité doit pouvoir effectuer plusieurs fonctions essentielles.

Bien que plusieurs outils pour la cybersécurité soient nécessaires pour satisfaire aux exigences de la solution CD-DAR, en théorie, les éléments ou composants clés fonctionnels recherchés peuvent être regroupés comme suit : [R31]

a. La capacité de maintenir la connaissance de la situation, au moyen d'une image commune de la situation opérationnelle, des alertes, des menaces et des mesures correctives dans l'ensemble du réseau de commandement du MDN et des FAC, et d'alimenter la connaissance de la situation aux fins de prise de décisions et l'exécution des interventions par des interfaces normalisées et des flux de travail automatisés à l'appui du soutien à la décision de l'élément de commandement, et la mise en œuvre des interventions selon les directives.

b. Capacité de créer et de tenir à jour un dépôt des cyberdonnées (CDR) faisant autorité qui comprend des données de cyberrenseignement multisources à intégrer (hébergées et exploitées avec des applications et un dépôt fiable) dans le réseau de commandement assigné en tant que système cohésif;

c. La capacité d'utiliser un outil automatisé de découverte de cyberentités et d'événements (CEED) afin d'identifier et de suivre rapidement tous les actifs (autorisés et non autorisés) connectés au réseau de commandement et d'évaluer leurs attributs en matière de vulnérabilité, de configuration, de risque et de conformité aux correctifs;

d. La capacité d'utiliser un outil automatisé de surveillance et mesures de cybersécurité (CSMA) afin d'identifier et de suivre rapidement tous les actifs (autorisés et non autorisés) connectés au réseau de commandement et d'évaluer leurs attributs en matière de vulnérabilité, de configuration, de risque et de conformité aux correctifs;

e. La capacité d'analyser la cyberdéfense et prendre en charge des décisions (CDADS) en vue de recueillir, de conserver et d'analyser continuellement des renseignements sur les cybermenaces dans l'environnement du réseau de commandement et de détecter et de caractériser les activités suspectes fournit un contexte pour les évaluations des risques et des vulnérabilités en temps quasi réel.

f. La capacité d'effectuer la gestion automatisée des tâches (GT) pour identifier, contenir et éradiquer une menace de façon adaptative et dynamique;

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

L'annexe A décrit chacun de ces éléments fonctionnels théoriques et la Figure 3 présente les interrelations entre les composantes fonctionnelles.

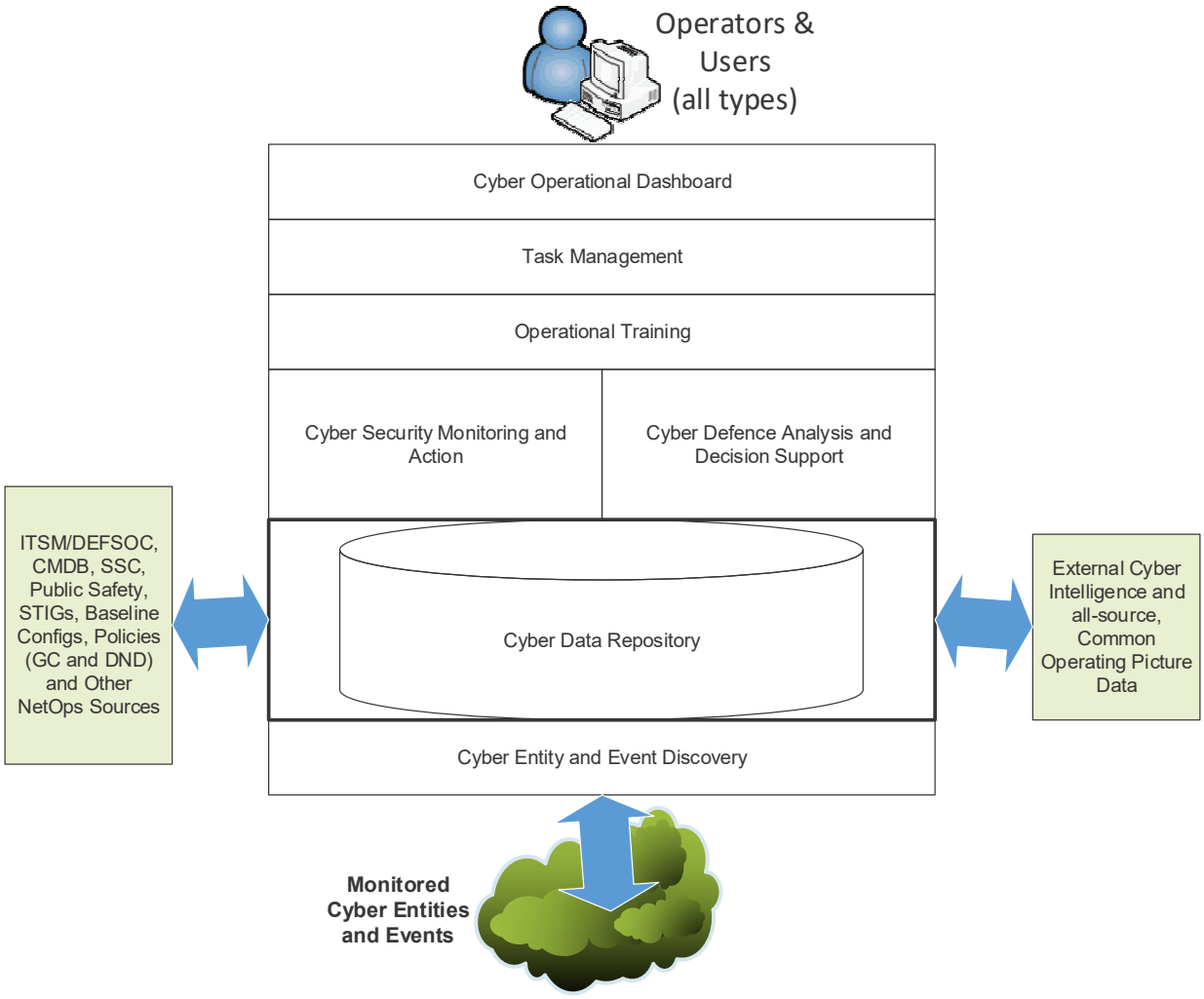


Figure 3 – Interrelations entre les composantes fonctionnelles de la solution CD-DAR

4. EXIGENCES EN MATIÈRE D'EFFICACITÉ DU SYSTÈME

4.1. Exigences générales

Cette section définit les exigences en matière d'efficacité du système pour la solution CD-DAR tel qu'elles sont comprises à ce stade de l'élaboration du projet. Ces exigences portent sur la capacité complète et doivent être définies plus en détail de concert avec le développement du CONOPS afin d'équilibrer les capacités technologiques disponibles lors de la mise en œuvre du projet avec le personnel et les procédures d'exploitation. Les exigences relatives à l'efficacité du système couvrent les domaines suivants :

a. exploitabilité;
b. surviabilité;
c. maintenabilité;
d. disponibilité;
e. fiabilité;
f. durabilité environnementale;
g. santé et sécurité;
h. exigences sur le plan de la livraison.

Les exigences en matière d'efficacité du système ont été saisies au chapitre 8 – Tableau des exigences du présent document et complétées par les exigences relatives aux objectifs de rendement (OREN) présentées à la section 6.

4.1.1. Niveaux de mesure des exigences et critères de performance

Deux niveaux de mesure définissent les différentes exigences en matière de rendement : essentiel ou souhaitable.

4.1.1.1. Exigence obligatoire

Une exigence obligatoire est un critère permettant de garantir la conformité de la solution CD-DAR avec les exigences minimales relatives à la performance et aux opérations. La performance ainsi décrite est jugée à ce point importante que si une solution proposée répond à tous les critères souhaitables et à tous les autres critères obligatoire sauf un, elle sera rejetée. Dans le présent document, le verbe devoir au présent (« doit ») désigne une exigence obligatoire.

4.1.1.2. Exigence souhaitable

Les exigences souhaitables servent à évaluer de façon plus approfondie des éléments de la solution qui satisfont à toutes les exigences obligatoire. Une exigence souhaitable décrit une exigence liée au rendement selon laquelle on considère qu'un rendement plus élevé que le niveau essentiel stipulé revêt une valeur opérationnelle importante. Dans le présent document, les verbes devoir au conditionnel (« devrait ») et pouvoir au conditionnel (« pourrait ») désignent une exigence souhaitable.

4.1.2. Avertissement concernant les niveaux de mesure

La stipulation d'un critère essentiel suppose que celui-ci est réalisable à un coût raisonnable. Toutefois, dans l'éventualité où une exigence essentielle serait jugée par la suite impossible à respecter pour des raisons techniques ou financières, elle sera réévaluée. Les critères de performance établis dans l'EBO ne peuvent être modifiés qu'avec l'approbation du directeur du projet, après consultation du gestionnaire du projet.

4.2. Opérabilité

La solution CD-DAR sera considérée comme opérationnelle lorsque les exigences fonctionnelles (section 8), les OREN (section 6) et les critères d'acceptation par l'utilisateur (section 4) auront été respectés.

4.3. Capacité de survie

La capacité doit être efficace dans tous les environnements opérationnels, comme il est indiqué à la section 2.2 du présent EBO, puisque la solution CD-DAR sera intégrée au réseau hôte en tant que capacité interne. Le système doit, dans la mesure du possible, être conçu pour résister aux menaces identifiées à la section 2.3 du présent EBO, grâce à l'utilisation de technologies adaptatives et d'analyses intégrées à la solution CD-DAR.

4.4. Maintenabilité

En tant que système primaire et critique pour le COD, la solution CD-DAR sera utilisée par les opérateurs cybernétiques, les gestionnaires, les cadres supérieurs et les autres opérateurs 24 heures sur 24, 7 jours sur 7. Les exigences relatives à la fiabilité, à la disponibilité et à la maintenabilité du système doivent répondre à ce besoin opérationnel et doivent être soutenues et entretenues conformément à la section 2.5 du CONSUP du présent EBO.

Le système doit être réparé et fonctionner comme il est déterminé par la catégorisation de sécurité (anciennement l'énoncé de sensibilité) et le processus d'autorisation et d'accréditation de sécurité (AAS). La catégorisation de la sécurité est un processus visant à déterminer les blessures attendues en raison de la compromission de la menace et le niveau de ces blessures prévues en ce qui concerne les objectifs de sécurité liés à la confidentialité, l'intégrité et la disponibilité. Une première itération de documents est effectuée pendant la phase de définition du projet, tandis que le processus d'AAS définit la gestion des risques liés à la sécurité des TI des systèmes d'information.

Le système doit utiliser des fonctions[11] de surveillance et de contrôle de la santé dans l'infrastructure existante des FAC pour surveiller et maintenir l'exploitation nominale de la solution CD-DAR.

L'architecture du système doit être conçue de manière à ce que chaque équipement puisse être réparé, entretenu et remplacé avec un impact minimal sur le fonctionnement de la capacité.

Les pannes prévues, nécessaires à l'entretien et à la mise à niveau planifiés du système, doivent être relativement rares et de courte durée. Afin de maintenir le rythme opérationnel, le système doit pouvoir être rétabli à sa configuration opérationnelle minimale (à définir plus tard) rapidement. Par conséquent, tous les efforts raisonnables doivent être faits pour rétablir la configuration opérationnelle minimale ou meilleure en raison d'une panne imprévue et menant à une exploitation nominale complète.

Cette capacité devrait être déployée sur des plates-formes matérielles de qualité commerciale standard. Ainsi, la configuration matérielle du système doit répondre aux exigences de maintenabilité pour ce matériel. De plus, tout logiciel de développement doit être élaboré à l'aide des pratiques exemplaires de l'industrie afin d'assurer un niveau élevé de fiabilité et de facilité d'entretien.

On s'attend à ce que la communauté d'utilisateurs et la fonctionnalité du système évoluent au fil du temps. Pour répondre au besoin d'évolution, le système doit appliquer les pratiques exemplaires et les lignes directrices de l'industrie afin de s'assurer que le logiciel et le système de la capacité sont :

a. Variable. L'ajout d'utilisateurs et/ou de points d'extrémités ne doit pas entraîner une dégradation inacceptable du rendement;

b. Extensible. L'intégration de fonctionnalités supplémentaires ne doit pas nécessiter de changements majeurs à l'architecture de la solution existante ou de ses composants/sous-composants individuels;

[11] Le terme « santé » renvoie ici au fonctionnement nominal du système de CD-DAR

c. Adaptables et modifiables. Les modifications apportées aux fonctionnalités existantes ne doivent pas nécessiter de modifications majeures à l'architecture de la solution existante ou de ses composants ou sous-composants individuels.

4.4.1. Acceptation par le personnel de maintenance

L'acceptation par le personnel de maintenance doit être obtenue avant l'acceptation finale de la capacité (telle que définie à la section 4.4). L'acceptation par le personnel de maintenance sera autorisée par le SMA(GI). Comme dans le cas de l'acceptation par l'utilisateur, l'acceptation par le personnel de maintenance doit se faire en deux phases :

a. acceptation de la COI;
b. acceptation de la COT.

L'acceptation par le personnel de maintenance à chaque phase nécessitera la réalisation d'une série d'activités, telles que définies dans les certificats de COI et de COT (à élaborer ultérieurement). À la fin de toutes les activités pour la COI ou la COT, le responsable de l'acceptation (SMA[GI]) doit soit « accepter entièrement », « refuser » ou « accepter avec conditions » la solution CD-DAR. Pour tout ce qui n'est pas une acceptation complète, l'autorité responsable de l'acceptation doit fournir des directives sur les mesures correctives nécessaires pour obtenir l'acceptation complète.

4.5. Disponibilité

Afin de maintenir le rythme opérationnel, le système doit pouvoir être rétabli à sa configuration opérationnelle minimale (à définir plus tard) rapidement. Par conséquent, tous les efforts raisonnables doivent être faits pour rétablir rapidement la configuration opérationnelle minimale ou meilleure en raison d'une panne imprévue et menant à une exploitation nominale complète. Les pannes prévues, nécessaires pour l'entretien et les mises à niveau prévues, doivent également être de courte durée.

La solution CD-DAR doit pouvoir effectuer une surveillance et une analyse localisées et appuyer la prise de décisions responsables au sein de réseaux régionaux déconnectés, intermittents et limités géographiquement, même lorsqu'il est déconnecté d'un point de gestion central. La solution CD-DAR déployée doit rendre le même niveau de disponibilité que la capacité durable lorsqu'elle fonctionne dans des environnements déconnectés, intermittents et limités géographiquement.

4.6. Fiabilité

Pour répondre à la disponibilité opérationnelle requise, la solution CD-DAR doit être hautement fiable, tel que défini par la disponibilité des capacités de CD-DAR, avec un taux de défaillance relativement faible.

4.7. Durabilité environnementale

La solution CD-DAR doit satisfaire aux normes de gérance environnementale du MDN. Le MDN et les FAC ont adopté le code de gérance environnementale suivant [R40]. Le MDN et les FAC doivent :

1. intégrer les facteurs environnementaux aux autres considérations pertinentes (opérations, finances, sécurité, santé, développement économique, etc.) qui entrent en ligne de compte dans la prise de décision;
2. respecter, sinon dépasser la lettre et l'esprit de la législation fédérale;
3. au sein du MDN et des FC, accroître le niveau de sensibilisation à l'environnement par des séances de formation, et favoriser et reconnaître les initiatives du personnel qui mènent à des effets positifs sur l'environnement;
4. reconnaître que le cycle de vie de la gestion des matières dangereuses (sélection initiale, acquisition, utilisation, manutention, entreposage, transport et élimination) est un facteur essentiel de toute planification,

particulièrement pour ce qui est de déterminer si l'acquisition des matières est vraiment nécessaire étant donné leurs caractéristiques (voir la DOAD 4003-1, *Gestion des matières dangereuses*);

5. assurer l'intégration des considérations environnementales dans les politiques et les pratiques en matière d'approvisionnement;
6. prendre des mesures pour prévenir la pollution associée aux activités et opérations quotidiennes par des moyens économiques de réduction de la consommation des matières premières, des substances toxiques, de l'énergie, de l'eau et d'autres ressources, et de diminution du volume des déchets et du bruit;
7. acquérir, gérer et aliéner les terres sans nuire à l'environnement, notamment en protégeant les aires écologiquement importantes.

4.8. Santé et sécurité

La solution 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. Elle doit être conforme avec tous les codes de santé et sécurité du MDN et des FAC.

4.9. Exigences sur le plan de la livraison

À déterminer

5. EXIGENCES EN MATIÈRE D'EFFICACITÉ DES SOUS-SYSTÈMES

S/O – Les niveaux des sous-systèmes ne sont pas définis avant la phase de définition du projet.

6. MESURES DE RENDEMENT

Les mesures de rendement sont présentées ci-dessous sous la forme de paramètres de rendement du système selon les conventions suivantes :

a. **Indicateur de rendement** : titre indiquant le type de mesure du rendement.
b. **Description du rendement** : une description de l'indicateur de rendement.
c. **Quantité (Qté)** : valeur de l'indicateur à atteindre.
d. **Unité de mesure** : unité dans laquelle la quantité est mesurée.

6.1. Mesures au niveau du système

Cette section présente une série d'indicateurs de rendement qui seront quantifiés à l'étape du projet de définition.

Tableau 5 – Paramètres de rendement du système [R2]

ID (objectif de rendement)	Indicateur de rendement	Description	Qté
OREN.1	Lien entre entités	Détecter qu'une cyberentité devient active (connectée) dans le cyberespace du MDN et des FAC. (p. ex., un ordinateur portable a été connecté au réseau, un utilisateur a ouvert une session, une clé USB a été branchée à un ordinateur, etc.).	À déterminer
OREN.2	Prévention automatique des attaques	Éviter automatiquement une attaque contre le réseau ou le processeur central par l'utilisation d'un outil de protection comme le système de prévention des intrusions sur l'hôte.	À déterminer
OREN.3	Entrée de vérification et affichage de la console GIES	Créer une entrée de vérification et l'envoyer à la console de gestion de l'information et des événements de sécurité (GIES).	À déterminer
OREN.4	Analyse automatique des anomalies des fichiers	Extraire automatiquement des fichiers d'une source, comme des pièces jointes d'un courriel ou un téléchargement du réseau, les exécuter dans une chambre de détonation et les analyser pour déceler des signes d'activités malveillantes.	À déterminer
OREN.5	Alerte automatique du SDI et affichage de la console	Déclencher une alerte dans le système de détection d'intrusion (SDI), puis envoyer l'alerte et les paquets associés à la console GIES.	À déterminer
OREN.6	Détection des attributs des entités	Déceler si la cyberentité détectée dans le cyberespace du MDN et des FAC est humaine ou non, et découvrir ses caractéristiques clés.	À déterminer
OREN.7	Identification et emplacement de l'entité	Cerner suffisamment de caractéristiques clés de la cyberentité détectée dans le cyberespace du MDN et des FAC pour déterminer son identité et sa position (physique et logique) précises.	À déterminer

ID (objectif de rendement)	Indicateur de rendement	Description	Qté
OREN.8	Caractérisation de l'intention	Établir la caractéristique opérationnelle précise de la cyberentité détectée dans le cyberespace du MDN et des FAC pour la classer comme amie, ennemie ou Inconnue afin d'appuyer une décision d'engagement.	À déterminer
OREN.9	Recherches et collecte de données mensuelles dans le système	Rechercher dans les registres mensuels pour tout système dans le cyberespace du MDN et des FAC et recueillir les résultats.	À déterminer
OREN.10	Corrélation entre entités malveillantes et alertes	Créer des tableaux croisés dynamiques pour aider les cyberopérateurs à identifier les entités avec un comportement malveillant similaire ou relié et avertir l'opérateur afin qu'il puisse amorcer des mesures d'intervention.	À déterminer
OREN.11	Récupération des captures de paquets d'une entité selon les critères	Extraire les captures de paquets (PCAP) indexées d'une semaine de la mémoire en ligne avec des critères liés à l'entité comme des adresses IP, noms d'hôte, ports, comptes d'utilisateurs ou contenu.	À déterminer
OREN.12	Reconnaissance de l'événement inquiétant et mesure	Reconnaître un événement inquiétant et le marquer comme anodin ou remplir un incident et l'envoyer au tiers 2.	À déterminer
OREN.13	Isolation de l'hôte infecté	Isoler un hôte infecté.	À déterminer
OREN.14	Identification et contact du propriétaire de l'incident	Déterminer, puis contacter l'administrateur de système, l'officier de la sûreté ou l'officier des opérations au site contenant le système lié à l'incident potentiel.	À déterminer
OREN.15	Déploiement du cycle de vie des SDI, à la flotte de capteurs	Développer, télécharger, mettre à l'essai et déployer les signatures SDI à une flotte de capteurs.	À déterminer
OREN.16	Élaboration d'un plan d'intervention de multiples systèmes ou comptes	Identifier, analyser et développer un plan d'intervention contre une intrusion dans de multiples systèmes ou comptes.	À déterminer

ID (objectif de rendement)	Indicateur de rendement	Description	Qté
OREN.17	Analyse de la charge utile des maliciels des niveaux 2 et 3	Fournir l'analyse de la charge utile pour une nouvelle souche de virus au tiers 2 et tiers 3.	À déterminer
OREN.18	Définition et rétablissement des flux de données en panne	Identifier et rétablir les capteurs ou les flux de données en panne.	À déterminer
OREN.19	Information des intervenants sur les incidents majeurs	Réunir les intervenants et les informer des détails de l'incident majeur en cours.	À déterminer
OREN.20	Signature de la flotte des SDI ou purge du contenu SIEM	Purger mensuellement/trimestriellement toutes les signatures déployées à la flotte SDI ou tout le contenu déployé à la console GIES.	À déterminer
OREN.21	Mise à l'essai et recommandation des correctifs majeurs	Mettre à l'essai et recommander des correctifs majeurs à l'entreprise.	À déterminer
OREN.22	Analyse et documentation du contenu sur les incidents graves	Analyser et documenter le contenu du système impliqué dans l'incident majeur tout en adhérant aux normes de la chaîne de possession légale. • Déployer une équipe d'intervention en cas d'incident. • Récupérer les données. • Trier les données.	À déterminer
OREN.23	Analyse criminalistique à distance	Extraire à distance les artéfacts criminalistiques à des fins d'analyse et de preuve. • Fichiers • Processus • Mémoire • Registre • Image du disque dur virtuel • Image du disque dur au niveau des bits	À déterminer
OREN.24	Évaluation de l'intention d'un adversaire	Évaluer les actions et les intentions potentielles d'un adversaire qui opère par des réseaux circonscrits.	À déterminer
OREN.25	Analyse, rapport et présentation	Rapporter les résultats d'analyse et présenter des preuves juridiquement recevables.	À déterminer

ID (objectif de rendement)	Indicateur de rendement	Description	Qté
OREN.26	Opérationnalisation du cycle de vie des outils d'analyse personnalisés	Développer, déployer et rendre opérationnel des outils adaptés complexes de détection et d'analyse comme ceux utilisés dans les scripts pour Perl et GIES.	À déterminer
OREN.27	Base de référence des COD du cycle de vie des IPO	Réviser, examiner et créer une base de référence pour une instruction permanente d'opérations (IPO) pour une opération de cybersécurité défensive interne.	À déterminer
OREN.28	Mise en pratique des nouvelles procédures	Exercer les nouvelles procédures durant les quarts de travail des cyberopérateurs.	À déterminer
OREN.29	Avis de menace et de vulnérabilité émergentes	Informer les cyberopérateurs des nouvelles menaces et vulnérabilités.	À déterminer
OREN.30	Opérationnalisation des nouvelles techniques de défense	Créer de nouvelles techniques de défense fonctionnelles avec les nouvelles tactiques, techniques et procédures.	À déterminer
OREN.31	Opérationnalisation des nouvelles techniques de défense fondées sur des outils	Créer de nouvelles techniques de défense fonctionnelles avec de nouveaux outils pour traiter les menaces nouvellement identifiées et priorisées.	À déterminer
OREN.32	Évolution de la posture de sécurité	Améliorer la posture de sécurité globale (politiques, processus, outils) du cyberespace vulnérable du MDN et des FAC pour traiter les menaces nouvellement identifiées et priorisées.	À déterminer
OREN.33	Perte de données	Aucune perte de paquets aux points de présence surveillés	À déterminer
OREN.34	Perte de données	Aucune perte de journal des événements	À déterminer
OREN.35	Perte de données	Aucune perte de renseignement	À déterminer
OREN.36	Intégrité des données	Intégrité des données vérifiables	À déterminer
OREN.37	Surveillance des données	Empêcher les adversaires de détecter (et d'éviter) la présence des capacités de surveillance.	À déterminer

ID (objectif de rendement)	Indicateur de rendement	Description	Qté
OREN.38	Livraison d'événements de données	Assurer la livraison entière des événements de sécurité des appareils finaux au centre d'opérations de cybersécurité défensive tout en les protégeant d'accès ou de modification non autorisés.	À déterminer
OREN.39	Capacité de survie	Appuyer la surviabilité de la cybersécurité et les capacités des COD, même lorsque certains secteurs du cyberespace sont compromis ou contestés.	Vrai
OREN.40	Protection de la divulgation des documents	Protéger des divulgations non autorisées des documents et des registres de nature délicate maintenus par les capacités des opérations de la cybersécurité défensive.	Vrai

6.2. Mesures du niveau des sous-systèmes

S/O – Les niveaux des sous-systèmes ne sont pas définis avant la phase de définition du projet.

7. BESOINS EN PERSONNEL ET EN ENTRAÎNEMENT

Pour être efficace, le système doit être exploité et soutenu par des ressources qualifiées affectées aux rôles clés, tels que définis à la section 2.6 ci-dessus.

La solution doit intégrer les pratiques exemplaires et mettre en œuvre l'apprentissage fondé sur les connaissances des opérations et mesures précédentes.

7.1. Besoins en personnel

La dotation de la solution CD-DAR comprendra le personnel militaire, les fonctionnaires et le personnel contractuel.

7.1.1. Employés opérationnels

Le système sera utilisé par le personnel du MDN et des FAC qui se voit attribuer des rôles et des pouvoirs d'utilisateur accrédités au sein de la solution CD-DAR. D'autres utilisateurs temporaires et permanents seront ajoutés au besoin pour répondre aux exigences en matière de saisie de données pour les opérations et pour répondre aux besoins en matière de transfert de matériel et de capacité de pointe pour la préparation et la clôture des missions. Le personnel opérationnel affecté à ces postes sera doté par Cyber Uplift.

7.1.2. Personnel d'entretien

Aux fins de l'analyse des options, on suppose que le système sera tenu à jour par le personnel du MDN et des FAC qui se voit attribuer la fonction de soutien respective à l'appui de la solution CD-DAR. Dans le cadre de la phase de définition, une analyse du SES sera menée, ainsi qu'une mobilisation continue de l'industrie, afin de déterminer une stratégie de maintenance qui offre le meilleur rendement, la souplesse et l'optimisation des ressources. Aujourd'hui, le CORFC est le gestionnaire du cycle de vie du matériel (GCVM) de facto pour la plupart des équipements et des logiciels cybernétiques existants.

7.2. Instruction

Afin de bien exploiter et soutenir la solution CD-DAR, un régime d'instruction efficace doit être fourni. L'instruction du cadre initial sera offerte dans le cadre de la portée du projet. Toutefois, l'instruction périodique sera donnée dans le cadre du SES de la capacité et sera la responsabilité de l'AO. L'AO peut déléguer au RT le pouvoir d'assurer la maintenance et la formation des administrateurs.

Le programme d'instruction sur la solution CD-DAR doit fournir une instruction supplémentaire sur le contenu du projet, fondée sur une approche d'instruction des formateurs, intégrée au programme d'instruction des COD du MDN et des FAC [R32].

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

7.2.1. Environnement de formation

La vision de la cyberdéfense sur le plan de l'analyse des décisions et de la réponse est un environnement intégré unique qui permet la collaboration et la conduite de la cybersécurité et des COD dans de multiples domaines de classification variable. Cela comprend, mais sans toutefois s'y limiter, les personnes, les politiques, les processus et les outils nécessaires à la visualisation, à la gestion des tâches, à l'instruction individuelle et collective et à un référentiel de données accessible et exploitable menant à un domaine cybernétique défendable du MDN et des FAC.

La solution doit fournir un SEO intégré pour s'assurer que les cyberopérateurs, les gestionnaires, les cadres et les autres opérateurs sont à jour et maîtrisent leurs tâches, rôles et responsabilités dans lsolution CD-DAR intégrée, y compris :

a. la capacité de créer une simulation de menace, de pénétration et d'attaque opérationnelle pour exercer l'équipe de cyberopérateurs et évaluer leur état de préparation opérationnelle ainsi que leur efficacité;

b. un composant d'entraînement opérationnel individuel axé sur les opérateurs individuels (tâches, rôles, progrès dans leur rôle);

c. une instruction axée sur les compétences et la validation des cyberopérateurs, opérateurs et civils dans leur rôle attribué autant au niveau individuel que collectif;

d. un composant d'instruction collective pour une capacité d'opération de sécurité pour la cyberdéfense. Ceci est une réplique d'un ensemble de systèmes d'exploitation avec des ensembles de données hors ligne pour permettre une gamme complète de fonctions et de scénarios réalistes à des fins de formation.

La solution doit dispenser une capacité de simulation d'instruction pour appuyer l'instruction opérationnelle collective dans un contexte opérationnel personnalisable. Les scénarios pour les simulations de formation doivent être créés, maintenus, modifiés et exécutés par les cyberopérateurs à partir des systèmes et des postes de travail actuels dans un environnement de formation ou d'exercice. La solution doit intégrer les pratiques exemplaires et mettre en œuvre l'apprentissage fondé sur les connaissances des opérations et mesures précédentes.

7.2.2. Produits livrables pour l'instruction

Ceux-ci comprendront, mais pourraient ne pas être limités aux :

a. Plans d'instruction et matériel d'instruction avec les outils en ligne dans le cyberespace du MDN et des FAC

   i. Instruction des membres du cadre initial d'instructeurs, axée à la fois sur l'instruction individuelle et collective des cyberopérateurs

   ii. Instruction continue, axée à la fois sur l'instruction individuelle et collective des cyberopérateurs.

b. La capacité du MODC sert à guider les cyberopérateurs pour améliorer leurs compétences et améliorer les cyberopérations des FAC afin d'assurer le maintien des compétences.

8. TABLEAU DES EXIGENCES

Les tableaux des exigences de cette section décrivent les exigences préliminaires pour atteindre les objectifs du projet de CD-DAR. Ils sont organisés en fonction du cadre d'analyse décrit à la Figure 4 ci-dessous. Le cadre a été élaboré à l'origine dans la version 1 du document d'architecture technique (DAT) et utilisé pour rédiger les exigences obligatoires de haut niveau (EOHN) pour la solution CD-DAR.

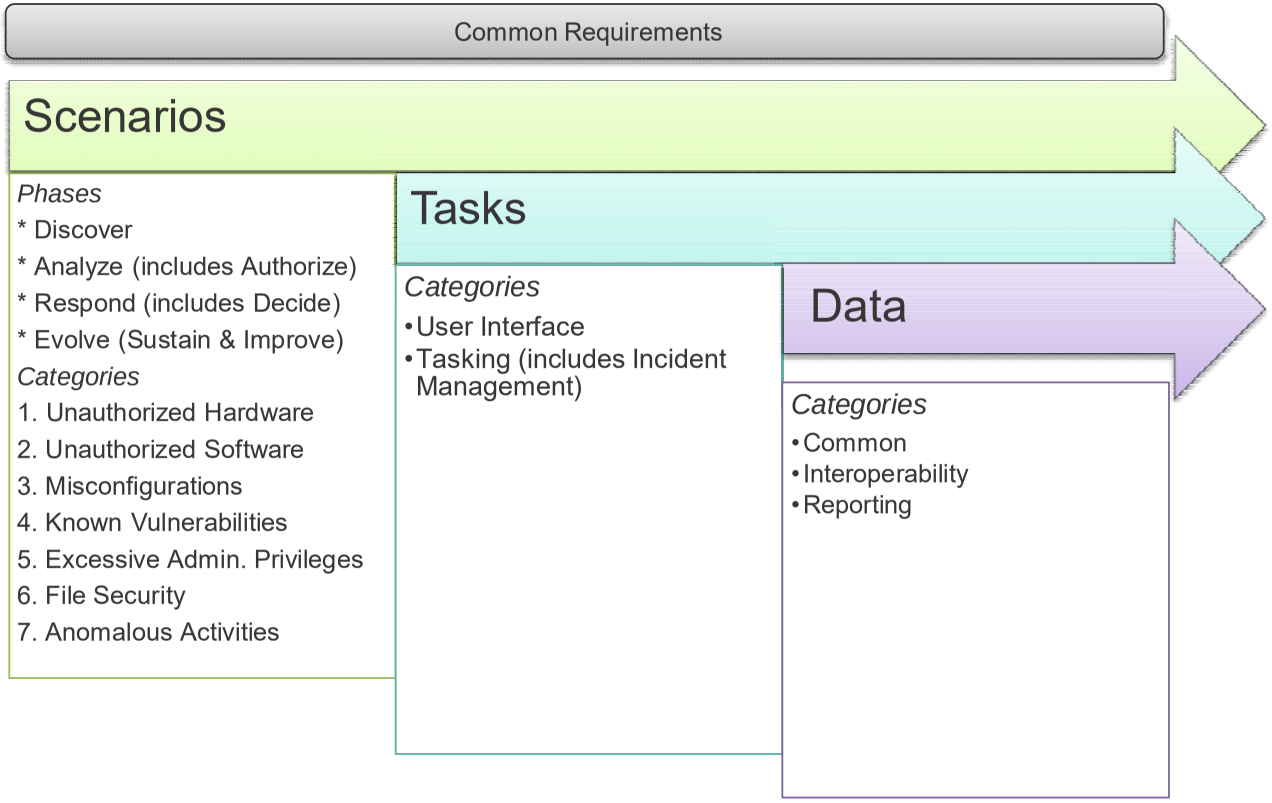


Figure 4 – Cadre d'analyse de CD-DAR

Figure 5 – Comparaison du cadre de CD-DAR

8.1. Exigences opérationnelles communes

Ce tableau comprend les exigences générales qui ne correspondent logiquement à aucune des autres catégories d'exigences plus précises.

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OCR-001	Gestion des réseaux	Le système doit appuyer les emplacements de réseau qui sont gérés par le MDN, les FAC ou des tiers, ou aux endroits où la gestion est partagée.	Exigence obligatoire	Exigence obligatoire	Tous
OCR-002	Contrôles de sécurité	La capacité doit tenir compte du contrôle de sécurité critique 1-5 du SCI de façon rapide et hautement automatisée.	Exigence obligatoire	Exigence obligatoire	Tous
OCR-003	Scénarios de domaine cybernétique	Le système doit être en mesure de traiter les scénarios suivants du domaine cybernétique : matériel non autorisé, logiciels non autorisés, erreurs de configuration, vulnérabilités connues, privilèges administratifs non autorisés, sécurité des dossiers et activités anormales.	Exigence obligatoire	Exigence obligatoire	Tous
OCR-004	Phases du cycle de vie	Le système doit fournir la fonctionnalité requise pour chacune des phases du cycle de vie de chaque scénario de domaine cybernétique, à savoir la découverte, l'analyse, l'intervention et l'évolution.	Exigence obligatoire	Exigence obligatoire	Tous
OCR-005	Mise en œuvre intégrée	Les capacités du projet doivent être intégrées aux capacités opérationnelles au moment de la mise en œuvre. Les exemples comprennent l'environnement de formation existant [surveillance et contrôle de la santé, SEO], les tâches d'aide à la décision et le chiffrement des données.	Exigence obligatoire	Exigence obligatoire	Tous
OCR-006	Gérance environnementale	Le système doit respecter les normes du MDN et des FAC relatives à la solution ADR. Les exemples comprennent la gérance environnementale et les codes de santé et de sécurité.	Exigence obligatoire	Exigence obligatoire	Tous

8.2. Exigences de découverte opérationnelle

Ce tableau comprend les exigences visant à déterminer l'état actuel de toutes les entités responsables des cyberactifs et de l'utilisation du réseau dans le cyberenvironnement, dont la plupart sont traitées automatiquement et rapidement. À noter que les exigences relatives au privilège administratif couvrent également les exigences relatives aux activités anormales.

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
		Découverte commune			
ODR-001	Découverte de l'entité	Le système doit fournir une identification et un suivi continus en temps réel des entités de cyberactifs et de l'utilisation du réseau.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-002	Découverte de l'état actuel	Le système doit fournir un processus et des outils automatisés pour l'intégration des ensembles de données et des métadonnées existants et nouvellement identifiés de l'état.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-003	Horodatage de la découverte	Le système doit comporter une date et une heure associées à chaque cas d'information sur l'état réel et indiquer la source de la collecte.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-004	Contexte de la découverte	Le système doit comprendre le mécanisme permettant de définir l'état réel en fonction du contexte et de la portée.	Exigence obligatoire	Exigence obligatoire	1.2
		Découverte de matériel			
ODR-005	Découverte de matériel	Le système doit identifier et suivre les dispositifs matériels (physiques et virtuels) qui sont sur le réseau, l'état d'autorisation et qui (individu, groupe d'accès ou organisation) gère chaque dispositif.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-006	Calendrier de découverte du matériel	Le système doit identifier et recueillir de l'information sur l'inventaire matériel de tous les appareils sur le réseau, de façon régulière et ponctuelle, selon les spécifications des utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-007	Identification du matériel	Le système doit fournir un identificateur unique (qui peut varier selon le type d'appareil) qui prend en charge les dispositifs persistants de tout changement d'emplacement réseau pour chaque dispositif sur le réseau.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-008	Emplacement du matériel	Le système doit recueillir des données pour permettre au personnel de localiser physiquement les dispositifs matériels.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-009	Information sur la validation du matériel	Le système doit recueillir des données matérielles supplémentaires (p. ex., sous-composants, périphériques joints, renseignements sur les comptes locaux) pour les dispositifs gérés et correctement configurés et avec des justificatifs suffisants pour valider les données d'inventaire réelles.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-010	Type de matériel axé sur le comportement	Le système devrait détecter le type de chaque dispositif matériel en fonction de son comportement réseau.	Exigence souhaitable	Exigence souhaitable	1.2

		Découverte de logiciels			
ODR-011	Découverte de logiciels	Le système doit identifier et suivre les produits logiciels qui se trouvent sur l'appareil pour chaque dispositif matériel (physique et virtuel) sur le réseau à l'intérieur des limites du système, de l'état d'autorisation, et qui (individu, groupe d'accès ou organisation) gère chaque produit logiciel.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-012	Identification du logiciel	Le système doit fournir un identificateur unique (p. ex., le dénombrement des plates-formes communes, les étiquettes d'identification de logiciel) pour chaque produit logiciel qui est utilisé pour identifier les instances des produits et composants logiciels installés, y compris le numéro de version, entre les appareils du réseau.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-013	Calendrier de découverte des logiciels	Le système doit identifier et recueillir des renseignements sur l'inventaire des logiciels définis et visés par le MDN et les FAC sur le réseau, de façon planifiée et ponctuelle, selon les spécifications des utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-014	Détails de la découverte de logiciels	Le système doit recueillir des données logicielles supplémentaires (p. ex., composants logiciels, empreintes numériques des composants) pour les dispositifs gérés et correctement configurés, avec des justificatifs d'identité suffisants pour valider les données d'inventaire réelles.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-015	Propriété et état du logiciel	Le système doit documenter et enregistrer l'information sur l'inventaire des logiciels, y compris le nom du produit, le propriétaire/gestionnaire et l'état opérationnel.	Exigence obligatoire	Exigence obligatoire	1.2
		Découverte de la configuration			
ODR-016	Découverte de la configuration	Le système doit déterminer et recueillir les paramètres de configuration (y compris les valeurs réelles) pour des logiciels et des produits matériels précis sur des dispositifs définis et visés par le MDN et les FAC sur le réseau, selon un calendrier établi, dicté par les événements, et ponctuel selon les spécifications des utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-017	Identification de la configuration	Le système doit prendre en charge un identificateur unique pour chaque collection de réglages de configuration de dispositifs sur le réseau.	Exigence obligatoire	Exigence obligatoire	1.2
		Découverte de vulnérabilités			
ODR-018	Découverte de vulnérabilités	Le système doit identifier et recueillir des renseignements sur les vulnérabilités, y compris la première fois où elles sont détectées et la première fois qu'elles sont corrigées, sur tous les appareils du réseau, selon un calendrier établi, en fonction des événements et de façon ponctuelle, tel que spécifié par les utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-019	Cartographie des vulnérabilités	Le système doit recueillir les données appropriées pour cartographier les vulnérabilités réelles des inventaires de matériel et de logiciels sur le réseau.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-020	Méthodes de découverte des vulnérabilités	Le système doit découvrir les vulnérabilités du réseau au moyen de méthodes non authentifiées ou authentifiées.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-021	Découverte de données sur les correctifs de vulnérabilité	Le système doit offrir un processus sécuritaire de gestion des correctifs qui assurera l'identification et l'acquisition automatique des correctifs pour tous les produits et les systèmes (commerciaux ou gouvernementaux).	Exigence obligatoire	Exigence obligatoire	1.2

ODR-022	Découverte de la portée sur les correctifs de vulnérabilité	Le système de gestion des correctifs doit être accessible à partir des emplacements, des biens et des utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	1.2
		Découverte d'accès administratif ou privilégié			
ODR-023	Renseignements sur la confiance des utilisateurs	Le système doit recueillir et communiquer des renseignements sur la confiance de tous les utilisateurs.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-024	Niveau de confiance réel de l'utilisateur	Le système doit déterminer le niveau de confiance accordé à chaque utilisateur autorisé.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-025	Niveau de confiance requis de l'utilisateur	Le système doit déterminer le niveau de confiance opérationnel requis pour chaque utilisateur.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-026	Renseignements réels sur l'instruction	Le système doit recueillir et signaler les renseignements sur l'instruction[12] pour chaque utilisateur autorisé au sein du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-027	Renseignements réels sur l'instruction	Le système doit comprendre l'instruction suivie, les connaissances démontrées et/ou la certification obtenue, selon la politique du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-028	Information sur l'instruction des utilisateurs	Le système doit prendre en charge la collecte, la surveillance et la déclaration de l'instruction générale en matière de sécurité qui s'applique à tous les utilisateurs.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-029	Renseignements sur l'instruction sur les rôles	Le système doit prendre en charge la collecte, la surveillance et la production de rapports pour l'instruction liée à la sécurité en fonction des rôles autorisés/attribués à l'utilisateur.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-030	Renseignements sur l'instruction complétée	Le système doit recueillir des données associées à l'instruction terminée et à la documentation sur les comportements liés à la sécurité requise pour les exigences en matière de comportement lié à la sécurité, pour lesquelles l'utilisateur est affecté ou autorisé, afin de fournir des éléments de données mesurables pour la création de vérifications de sécurité automatisées.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-031	Instruction terminée au niveau du processus	Le système doit générer des rapports sur la réussite de l'instruction indispensable offerte aux systèmes et aux processus qui peuvent surveiller et appliquer l'accès.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-032	Renseignements sur les justificatifs d'identité de l'employé	Le système doit recueillir et déclarer les renseignements sur les justificatifs d'identité associés aux comptes et aux justificatifs d'identité des utilisateurs (p. ex., certificats X.509, identificateurs d'utilisateur, paires de clés publiques/privées) délivrés à chaque utilisateur employé par le MDN ou les FAC (y compris les entrepreneurs).	Exigence obligatoire	Exigence obligatoire	1.2
ODR-033	Changements de justificatifs d'identité	Le système doit recueillir et déclarer les renseignements sur les justificatifs associés à la réémission, à la révocation et à la suspension des justificatifs d'identité des comptes et des utilisateurs, ainsi que leur configuration pour tous les types de justificatifs applicables.	Exigence obligatoire	Exigence obligatoire	1.2

[12] L'instruction comprend : la formation, les connaissances et/ou la certification, selon la politique du MDN et des FAC.

ODR-034	Complexité des mots de passe d'attestation	Le système doit recueillir et déclarer les renseignements sur les justificatifs associés aux mécanismes d'application de la complexité des mots de passe des comptes et des utilisateurs et leur configuration pour tous les comptes visés au sein du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-035	Privilèges d'utilisateur et de compte	Le système doit recueillir et déclarer des renseignements sur les comptes et les utilisateurs privilégiés et non privilégiés.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-036	Privilèges d'accès physique	Le système doit recueillir et déclarer les autorisations d'accès physique délivrées à chaque utilisateur employé par le MDN et les FAC.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-037	État du compte	Le système doit recueillir et déclarer l'état du compte (restrictions, habilitation, révocation, période d'autorisation, etc.) mis en œuvre pour chaque compte visé au sein du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2
		Découverte de fichier			
ODR-038	Découverte sur le contrôle des documents	Le système doit automatiquement surveiller le réseau pour y repérer les étiquettes de données du MDN et des FAC sur certains types de fichiers afin de soutenir l'inventaire des fonds de données.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-039	Découverte de chaîne de possession numérique	Les technologies et processus du système doivent recueillir de l'information sur les exigences d'enquête du GC pour la chaîne de possession numérique.	Exigence obligatoire	Exigence obligatoire	1.2
		Découverte d'activités anormales			
ODR-040	Découverte des activités de l'utilisateur	Le système doit assurer la surveillance continue en temps réel des activités de l'utilisateur.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-041	Découverte du trafic sur le réseau	Le système doit assurer une surveillance continue en temps réel du trafic sur le réseau.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-042	Données de captures de paquets	Le système doit intégrer les données du PCAP.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-043	Découverte du trafic sur le réseau hors bande	Le système doit fournir toutes les données recueillies (hors bande) et conservées du trafic du réseau brut du cyberespace des FAC (interne, entrant, sortant).	Exigence obligatoire	Exigence obligatoire	1.2
ODR-044	Rétention du trafic sur le réseau.	Le système doit respecter les lignes directrices suivantes en matière de rétention des données : Alertes SDI et alertes connexes GIES :	Exigence obligatoire	Exigence obligatoire	1.2
ODR-045	Découverte des points d'extrémités	Le système doit fournir une capacité de détection et d'intervention des points d'extrémités (DIPE) pour identifier l'installation de logiciels malveillants sous forme de MPA sur un dispositif de point d'extrémité.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-046	Détails de la découverte des points d'extrémités	Le système doit offrir une capacité de cueillette des données détaillées concernant l'état actuel de chaque appareil d'extrémité (comme les processus en cours d'exécution, les réglages de registres, les fichiers actuellement ouverts, les connexions actives au réseau, le compte d'utilisateur en cours d'utilisation et les détails matériels comme l'utilisation de la mémoire et de l'UC).	Exigence obligatoire	Exigence obligatoire	1.2

ODR-047	Découverte de données des points d'extrémités	Le système doit offrir une capacité de cueillette à distance des images de la mémoire ou des fichiers pour une enquête judiciaire.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-048	Découverte de disque dur des points d'extrémités	Le système doit offrir une capacité de cueillette à distance des images du disque dur (serveur, poste de travail ou portable) pour une enquête judiciaire.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-049	Découverte de données d'interconnexion de réseaux	Le système doit recueillir et communiquer l'information relative à la mise en œuvre de politiques qui contrôlent le flux de données entre les enclaves à un ou plusieurs niveaux de la pile de protocoles. Ces renseignements doivent appuyer l'application de ces politiques.	Exigence obligatoire	Exigence obligatoire	1.2
ODR-050	Découverte de renseignement de sources ouvertes	Le système doit incorporer les flux de service cybernétique de renseignement de sources ouvertes (OSINT) durable, ajustable et de bonne réputation.	Exigence obligatoire	Exigence obligatoire	1.2

8.3. Exigences d'analyse opérationnelle

Ce tableau comprend les exigences visant à déterminer et à recommander des mesures à prendre en cas de conditions de sécurité et de défense non autorisées. Les exigences sont ensuite regroupées dans les sous-catégories suivantes :

1. *Autorisation*. Exigences pour faire la distinction entre les conditions autorisées et non autorisées.
2. *Détection*. Exigences pour déceler les conditions non autorisées et de recommander des mesures à prendre.
3. *Priorisation*. Exigences pour faciliter l'établissement des priorités des interventions.

À noter que les exigences relatives au privilège administratif couvrent également les exigences relatives aux activités anormales.

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
		Analyse commune			
OAR-001	Analyse du soutien aux décisions	Le système doit permettre d'exécuter des tâches de soutien aux décisions.	Exigence obligatoire	Exigence obligatoire	1.2
		Autorisation commune			
OAR-002	État faisant autorité	Le système doit comprendre le mécanisme permettant de définir l'état souhaité pour une entité dépendant du contexte de l'entité (p. ex., lien entre l'unité organisationnelle et le système) et la portée des attributs de la capacité.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-003	Analyses des données d'entreprise	Le système doit pouvoir faire l'analyse des données d'entreprise.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-004	Données d'EAS faisant autorité	Le système doit intégrer les données d'évaluation et d'autorisation de sécurité.	Exigence obligatoire	Exigence obligatoire	1.2

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OAR-005	Modifications de données autorisées	Le système doit fournir un processus et des outils automatisés pour l'intégration des ensembles de données et des métadonnées faisant autorité existants et nouvellement identifiés.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-006	Modifier les données autorisées	Le système doit développer des données faisant autorité pour soutenir l'identification automatisée des entités modifiées.	Exigence obligatoire	Exigence obligatoire	1.2
		Autorisation de matériel			
OAR-007	Matériel autorisé	Le système doit documenter et enregistrer les renseignements sur l'inventaire matériel approuvés par le MDN et les FAC (c.-à-d. les dispositifs autorisés), y compris le type d'appareil (p. ex., routeur, poste de travail, pare-feu, imprimante), le propriétaire ou le gestionnaire et l'état opérationnel.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-008	Méthodes d'entrée matériel autorisées	Le système doit permettre la création manuelle ou par lots de données sur les dispositifs approuvées par le MDN et les FAC (p. ex., par l'intégration avec des dépôts externes d'information sur les actifs ou au moyen de règles opérationnelles).	Exigence obligatoire	Exigence obligatoire	1.2
		Autorisation de logiciel			
OAR-009	Données logicielles autorisées	Le système doit établir et tenir à jour un inventaire des logiciels, des identificateurs uniques pour les logiciels et d'autres propriétés comme le gestionnaire du logiciel.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-010	Méthodes d'entrée logicielle autorisées	Le système doit permettre la création manuelle ou par lots de données logicielles autorisées (p. ex., par l'intégration avec des dépôts externes d'information sur les actifs ou au moyen de règles opérationnelles).	Exigence obligatoire	Exigence obligatoire	1.2
		Autorisation de configuration			
OAR-011	Configuration autorisée	Le système doit créer, mettre à jour et tenir à jour les paramètres de configuration de sécurité des dispositifs matériels et des produits logiciels cibles.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-012	Détails de la configuration autorisée	Le système doit stocker, traiter, tenir à jour, suivre les changements et distribuer les repères de configuration de sécurité, y compris les exceptions du MDN et des FAC (y compris les justifications et les contre-mesures de compensation), tel que déterminé par les utilisateurs autorisés (avec autorisation accordée par point de repère).	Exigence obligatoire	Exigence obligatoire	1.2
OAR-013	Renseignements de configuration autorisée	Le système doit permettre aux utilisateurs autorisés de sélectionner et de composer un ensemble de repères de configuration de sécurité afin d'établir une configuration de base de sécurité autorisée pour une entité responsable des cyberactifs ou un groupe d'actifs.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-014	Configurations de niveau d'actif autorisées	Le système doit enregistrer les paramètres de configuration de sécurité autorisés qui sont établis et gérés par des utilisateurs autorisés selon les repères définis pour les produits logiciels et matériels particuliers.	Exigence obligatoire	Exigence obligatoire	1.2

		Autorisation de vulnérabilité			
OAR-015	Vulnérabilités autorisées	Le système doit fournir des données faisant autorité sur les vulnérabilités grâce à une couverture complète des VEF identifiée par la base de données nationale sur les vulnérabilités (BDNV) et des renseignements équivalents sur les vulnérabilités provenant d'autres sources utiles.	Exigence obligatoire	Exigence obligatoire	1.2
		Autorisation du privilège administratif			
OAR-016	Identité de l'administrateur autorisé	Le système doit intégrer les données d'identité de l'administrateur accrédité.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-017	Identité de l'utilisateur faisant autorité	Le système doit intégrer les données d'identité de l'utilisateur accrédité.	Exigence obligatoire	Exigence obligatoire	1.2
	Données ministérielles d'authentification faisant autorité	Le système doit s'appuyer sur les capacités ministérielles en matière d'authentification et de justificatifs d'identité.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-018	Niveau de confiance de l'autorisation d'accès	Mettre les attributs d'autorisation de niveau de confiance clé à la disposition des systèmes et des processus qui surveillent l'accès.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-019	Exigences en matière de confiance pour l'accès des utilisateurs	Fournir, pour contrôler les systèmes et les processus qui surveillent l'accès, des attributs de confiance clés au sujet des exigences d'autorisation concernant un utilisateur au moment où l'utilisateur est autorisé à accéder à une installation ou à un compte dans un système.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-020	Comportement de l'utilisateur non autorisé	Le système doit fournir des mécanismes ou des processus de collecte pour détecter et enregistrer/signaler l'information afin de déterminer si un utilisateur autorisé ne répond pas aux exigences de comportement de sécurité fondées sur les attributs, et lorsque les exigences relatives aux comportements liés à la sécurité d'un utilisateur autorisé ont expiré.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-021	Exigences en matière de formation pour l'accès des utilisateurs	Le système doit fournir, pour contrôler les systèmes et les processus qui surveillent l'accès, des attributs de formation clés concernant les exigences d'autorisation concernant un utilisateur au moment où l'utilisateur est autorisé à accéder à une installation ou à un compte dans un système.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-022	Exigences relatives aux justificatifs d'accès d'un utilisateur	Le système doit fournir, pour contrôler les systèmes et les processus qui surveillent l'accès, des attributs de justificatifs clés au sujet des exigences d'autorisation concernant un utilisateur au moment où celui-ci est autorisé à accéder à une installation ou à un compte dans un système.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-023	Types de justificatifs d'identité de données	Le système doit utiliser un processus approuvé pour la délivrance de différents types de justificatifs d'identité et la définition des politiques sur les exigences d'authentification pour l'accès à diverses installations, systèmes et renseignements.	Exigence obligatoire	Exigence obligatoire	1.2
		Autorisation des dossiers			
OAR-024	Gestion des documents autorisés	Le système doit fournir des données autorisées pour l'étiquetage des données du MDN et des FAC sur des types de fichiers précis afin d'appuyer les vérifications de la conformité aux politiques de sécurité.	Exigence obligatoire	Exigence obligatoire	1.2

		Autorisation d'activités anormales			
OAR-025	Découverte du chiffrement d'interconnexion de réseaux	Le système doit recueillir des données associées à la politique de chiffrement des limites et à la politique de chiffrement requise pour un flux réseau à travers une limite afin de fournir des éléments de données mesurables pour la création de contrôles de sécurité automatisés.	Exigence obligatoire	Exigence obligatoire	1.2
		Détection courante			
OAR-026	Détection des biens non autorisés	Le système doit détecter les conditions non autorisées de l'entité responsable des cyberactifs (c.-à-d. matériel et logiciels non autorisés, erreurs de configuration, vulnérabilités connues et privilèges administratifs non autorisés) et les activités anormales.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-027	Analyse de sources multiples	Le système doit pouvoir pouvoir corréler des sources de données multiples et des processus d'évaluation d'appui par l'entremise de rapports et de requêtes sur mesure préfabriqués.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-028	Analyse des points de décision	Le système doit soutenir la corrélation entre l'entité responsable des cyberactifs et l'information sur l'utilisation du réseau, conjointement avec les points de décision, propres à la détermination de la fonction de l'état réel par rapport à l'état souhaité du point de décision.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-029	Corrélation de données faisant autorité	Le système fournira un moyen automatisé de relier des données faisant autorité provenant de sources multiples de façon prédéfinie.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-030	Intégration de la menace	Le système doit avoir une capacité automatisée, efficace et fiable de fusion des renseignements sur les menaces qui permet l'analyse de sources et de conditions multiples.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-031	Détection des données de modification	Le système doit identifier automatiquement les entités modifiées.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-032	Qualité et confidentialité des données	Dans chaque champ de données ou attribut recueilli, stocké ou déduit par analyse, un facteur de mérite de qualité et confidentialité des données est requis pour permettre une prise de décision judicieuse.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-033	Alertes d'analyse cybernétique	Le système doit fournir une méthode de création, de modification, de suppression, de visualisation et d'envoi des alertes.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-034	Données GIES autorisées	Le système doit intégrer les données GIES pour tous les scénarios du domaine cybernétique.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-035	Compromission liée à une mauvaise configuration	Le système doit pouvoir détecter les indicateurs de compromission.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-036	Évaluation du point de décision	Le système doit comprendre des capacités de prise de décision pour appuyer l'intégration de politiques lisibles par machine afin de mesurer l'état réel par rapport à l'état souhaité pour l'évaluation continue des contrôles de sécurité.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-037	Données de renseignements sur les menaces faisant autorité	Le système doit intégrer les données de renseignements sur les menaces.	Exigence obligatoire	Exigence obligatoire	1.2

OAR-038	Planification de l'évaluation de l'interface	Le système doit permettre des évaluations établies ou sur demande.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-039	Demandes d'évaluation de l'interface	Le système doit offrir un processus et des outils automatisés pour demander une évaluation sur mesure.	Exigence obligatoire	Exigence obligatoire	1.2
OIR-040	Conservation des résultats de l'évaluation	Le système doit conserver les résultats d'évaluation pour une période définie par le MDN et les FAC afin de permettre la production de rapports sur la posture de sécurité d'entreprise et l'établissement de tendances.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-041	Analyse rétrospective et vérifications	Le système doit appuyer les analyses rétrospectives et les fonctions de vérification.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-042	Rapports historiques	Le système doit offrir des analyses sur mesure des données antérieures à court terme (p. ex. : requête rédigée, modélisation de cas) qui appuie la capacité d'enregistrer les observations, de déclencher les alertes, puis de générer des comptes rendus.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-043	Corrélation historique	Le système doit fournir une corrélation entre les événements antérieurs, les tendances et les comportements, et les événements en temps réel afin de reconstruire les activités selon le contexte.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-044	Vérifications historiques	Le système doit fournir des outils de vérification qui appuient les requêtes et des rapports manuels et automatisés (prévus ou ponctuels).	Exigence obligatoire	Exigence obligatoire	1.2
OAR-045	Intégration des systèmes de contrôle des accès physiques	Le système doit intégrer les composants des systèmes de contrôle des accès physiques (PACS) adressables par IP pour soutenir toutes les capacités de CD-DAR.	Exigence obligatoire	Exigence obligatoire	1.2
		Détection du matériel			
OAR-046	Analyse matérielle	Le système doit recueillir les données appropriées pour établir une correspondance entre les données réelles et l'inventaire du matériel approuvé par le MDN et les FAC (c.-à-d. les appareils autorisés), y compris le moment où l'équipement est détecté et si l'appareil est dans l'état souhaité.	Exigence obligatoire	Exigence obligatoire	1.2
		Détection logicielle			
OAR-047	Analyse logicielle	Le système doit détecter l'exécution de logiciels non autorisés en les bloquant en fonction d'une liste de logiciels autorisés propre à chaque dispositif matériel. Au minimum, les exécutables résidents doivent être bloqués.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-048	Détection des changements de logiciel	Le système devrait détecter les changements de liste blanche et les mesures d'installation du logiciel.	Exigence souhaitable	Exigence souhaitable	1.2
OAR-049	Vérification de l'intégrité des sources de logiciels	Le système devrait fournir une vérification de l'intégrité de la source pour tous les composants de l'outil, comme les empreintes digitales numériques pour chaque fichier logiciel utilisé dans le système.	Exigence souhaitable	Exigence souhaitable	1.2

OAR-050	Détection et protection contre les logiciels malveillants	Le système devrait effectuer la détection des logiciels malveillants et assurer la protection contre ces derniers (y compris, selon la configuration, tous les logiciels sur liste blanche et les logiciels qui ne se comportent pas comme prévu) à un taux comparable à celui des logiciels antivirus, et fournir un moyen de retirer les logiciels malveillants à temps pour éviter qu'ils ne soient exécutés.	Exigence souhaitable	Exigence souhaitable	1.2
		Détection de la configuration			
OAR-051	Analyse de la configuration de sécurité	Le système doit énumérer les différences par rapport au point de repère de configuration de sécurité, y compris les différences qui offrent une protection plus grande ou réduisent le risque plus que le point de repère.	Exigence obligatoire	Exigence obligatoire	1.2
		Détection des vulnérabilités			
OAR-052	Incidences des vulnérabilités	Le système doit offrir un processus et des outils automatisés pour évaluer l'incidence des vulnérabilités connues (p. ex. les données sur les expositions et les vulnérabilités communes) des entités responsables des cyberactifs.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-053	Portée de l'incidence des vulnérabilités	L'évaluation de l'incidence des vulnérabilités du système doit inclure le type d'entité et la configuration du système complet ou de la fonction.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-054	Chaîne de destruction des vulnérabilités	L'évaluation de l'incidence des vulnérabilités du système doit inclure la chaîne de cyberdestruction au complet.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-055	Probabilité de compromission des vulnérabilités	L'évaluation de l'incidence des vulnérabilités du système doit déterminer la possibilité que le système soit compromis.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-056	Analyse des correctifs	L'évaluation de l'incidence des vulnérabilités du système doit automatiquement évaluer la nécessité d'installer des correctifs sur les actifs de réseau.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-057	Détection des vulnérabilités	Le système doit mettre à jour les outils en temps opportun afin de pouvoir détecter les vulnérabilités qui ont été identifiées par les VEF du gouvernement.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-058	Rapports sur les vulnérabilités	Le système doit produire des rapports d'évaluation des vulnérabilités.	Exigence obligatoire	Exigence obligatoire	1.2
		Détection des privilèges administratifs			
OAR-059	Analyse de la confiance des utilisateurs	Le système doit déterminer à quel moment un justificatif délivré par un utilisateur ne répond pas aux exigences relatives au niveau de confiance et à quel moment le niveau de confiance de cet utilisateur est expiré.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-060	Présélection du niveau de confiance de l'utilisateur	Le système doit utiliser un processus de présélection/d'endoctrinement établi avant d'accorder l'accès à divers niveaux de matériel sensible.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-061	Automatisation des vérifications de sécurité	Effectuer des vérifications de sécurité qui jettent les bases de l'automatisation de la surveillance, de la production de rapports et de la priorisation des lacunes de confiance dans le cyberenvironnement du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2

OAR-062	Comportement des utilisateurs autorisés	Le système doit recueillir et signaler les indicateurs de comportement liés à la sécurité pour chaque utilisateur autorisé au sein du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-063	Validation de la politique d'instruction des utilisateurs	Le système doit valider l'existence des politiques d'instruction du MDN et des FAC et rendre compte de leur application. Les politiques d'instruction du MDN et des FAC doivent documenter la durée de validité d'une activité d'instruction, de connaissances ou de certification avant son expiration et l'utilisateur doit répéter la formation, les connaissances ou la certification.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-064	Automatisation des tâches liées aux activités des utilisateurs	Le système doit utiliser des vérifications de sécurité automatisées pour fournir la base permettant d'identifier, de surveiller, de signaler, d'établir des priorités et d'examiner automatiquement les lacunes en matière de comportement liées à la sécurité dans le cyberenvironnement du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-065	Période de grâce pour l'instruction	Le système devrait définir des périodes de grâce appropriées pour l'instruction associée à chaque exigence comportementale liée à la sécurité.	Exigence souhaitable	Exigence souhaitable	1.2
OAR-066	Authentification de l'utilisateur	Le système doit vérifier les mécanismes d'authentification mis en œuvre pour chaque compte visé du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-067	Vérification des comptes d'utilisateur	Le système doit vérifier que les comptes/mots de passe par défaut ne sont PAS activés dans les systèmes visés.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-068	Validation du processus des justificatifs d'identité d'utilisateur	Le système doit surveiller continuellement les extrants clés des processus d'émission et de définition des justificatifs d'identité afin de détecter les cas où un justificatif ou une action d'authentification s'écarte des normes établies.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-069	Authentification des politiques	Le système doit s'assurer que tous les mécanismes d'authentification déployés sur les systèmes visés à l'échelle du MDN et des FAC mettent en œuvre la politique d'authentification appropriée.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-070	Validation des types de justificatifs d'identité d'utilisateur	Le système doit vérifier que tous les types de justificatifs d'identité ont des politiques appropriées d'expiration, de réémission et de révocation.	Exigence obligatoire	Exigence obligatoire	1.2
		Détection des fichiers			
OAR-071	Autorisation de l'étiquette de données	Le système doit évaluer les renseignements figurant sur les étiquettes de données de certains types de fichiers pour appuyer les vérifications de la conformité aux politiques de sécurité.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-072	Processus de chaîne de possession numérique	Les technologies et processus du système doivent vérifier la conformité aux exigences d'enquête du GC pour la chaîne de possession numérique.	Exigence obligatoire	Exigence obligatoire	1.2
		Détection des activités anormales			
OAR-073	Détection des activités anormales	Le système doit permettre de détecter les activités anormales.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-074	Autorisation d'activités anormales	Le système doit intégrer des données de base qui permettent de détecter les conditions acceptables et inacceptables du trafic sur le réseau et l'activité des utilisateurs.	Exigence obligatoire	Exigence obligatoire	1.2

OAR-075	Analyse des anomalies historiques	Le système doit fournir une analyse des données d'entreprise pour détecter des activités suspectes ou anormales.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-076	Détection avancée des menaces	Le système doit fournir les caractéristiques et les données pour appuyer la chasse aux menaces persistantes avancées (MPA), aux menaces intérieures et aux indicateurs.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-077	Capacités de détection des points d'extrémités	Le système doit fournir une capacité de détection et d'intervention des points d'extrémités (IPE) pour analyser la présence de logiciels malveillants sous forme de MPA sur un dispositif de point d'extrémité.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-078	Données criminalistiques	Le système doit intégrer des données criminalistiques.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-079	Données criminalistiques des points d'extrémités	Le système doit offrir une capacité de cueillette des données criminalistiques des appareils d'extrémités (comme les processus exécutés, les fichiers ouverts et créés, les applications/commandes/scripts utilisés, les comptes d'utilisateur utilisés et les applications installées).	Exigence obligatoire	Exigence obligatoire	1.2
OAR-080	Analyse des activités de l'utilisateur	Le système doit offrir l'analyse continue en temps réel des activités contextualisées de l'utilisateur.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-081	Corrélation des activités de l'utilisateur	Le système doit corréler l'activité de l'utilisateur entre les domaines et les oppositions.	Exigence obligatoire	Exigence obligatoire	1.2
		Priorisation commune			
OAR-082	Priorisation des tâches	Le système doit offrir un indicateur de priorité pour les tâches d'atténuation actuelles.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-083	Gestion des risques	Le système doit soutenir les processus et les outils permettant de déterminer, de définir, d'intégrer et d'automatiser continuellement la gestion des risques dans le domaine cybernétique du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	1.2
OAR-084	Détails de la gestion des risques	Les processus et les outils de gestion des risques doivent inclure la catégorisation des renseignements, la sélection de contrôle de sécurité, l'évaluation des mesures de sécurité, la vérification de conformité de la configuration et le calcul du risque.	Exigence obligatoire	Exigence obligatoire	1.2
OIR-085	Cotes de gestion des risques	Le système doit comprendre le mécanisme permettant de définir les cotes de risque pour la différence entre les états réels et les états souhaités (y compris les cotes qui reflètent une réduction du risque).	Exigence obligatoire	Exigence obligatoire	1.2
OAR-086	Criticité des actifs	Le système doit appuyer l'établissement des priorités des mesures correctives en identifiant les entités responsables des cyberactifs critiques.	Exigence obligatoire	Exigence obligatoire	1.2

8.4. Exigences de l'intervention opérationnelle

Ce tableau comprend les exigences nécessaires aux interventions en cas de conditions de sécurité et de défense non autorisées.

À noter que les exigences relatives au privilège administratif couvrent également les exigences relatives aux activités anormales.

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
		Intervention commune			
ORR-001	Intervention liée au plan d'urgence	Le système doit avoir un plan d'urgence pour restaurer et reconstituer toutes les fonctionnalités du système d'information et la capacité d'appliquer des mesures de sécurité nouvelles ou supplémentaires pour prévenir toute compromission future.	Exigence obligatoire	Exigence obligatoire	3
ORR-002	Intervention liée à la gestion des risques	Le système doit soutenir les processus et les outils pour les mesures automatisées d'intervention en matière de gestion des risques.	Exigence obligatoire	Exigence obligatoire	3
ORR-003	Réponses aux événements	Le système doit pouvoir régler l'intervention automatique à un événement.	Exigence obligatoire	Exigence obligatoire	3
ORR-004	Automatisation d'intervention prédéterminée	Le système doit permettre l'exécution automatique d'interventions techniques prédéterminées pour des événements documentés qui dépassent les seuils documentés.	Exigence obligatoire	Exigence obligatoire	3
ORR-005	Dérogation prédéterminée de l'intervention	Le système doit offrir une commande manuelle prioritaire pour les interventions préautorisées.	Exigence obligatoire	Exigence obligatoire	3
ORR-006	Intervention liée à la segmentation des infrastructures	Le système doit comprendre des outils automatisés afin de segmenter en temps opportun des parties de l'infrastructure avec des vulnérabilités nouvellement identifiées en matière de sécurité.	Exigence obligatoire	Exigence obligatoire	3
ORR-007	Intervention de filtrage	Le système doit appliquer une ou plusieurs politiques de filtrage en utilisant un ou plusieurs points de décision. Ces politiques de filtrage contrôlent les données qui peuvent entrer dans les systèmes ou en sortir.	Exigence obligatoire	Exigence obligatoire	3
		Intervention matérielle			
ORR-008	Intervention matérielle non autorisée	Le système doit fournir un processus et des outils automatisés pour réagir à la détection de conditions matérielles cybernétiques non autorisées.	Exigence obligatoire	Exigence obligatoire	3
		Intervention logicielle			
ORR-009	Intervention logicielle non autorisée	Le système doit fournir un processus et des outils automatisés pour réagir à la détection de conditions de cyberlogiciels non autorisées.	Exigence obligatoire	Exigence obligatoire	3
ORR-010	Intervention liée au changement de la liste blanche	Le système doit assurer la protection contre les changements de liste blanche et les mesures d'installation du logiciel.	Exigence obligatoire	Exigence obligatoire	3

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
ORR-011	Intervention liée à l'exécution des logiciels non autorisés	Le système doit assurer la protection contre l'exécution de logiciels non autorisés en les bloquant en fonction d'une liste de logiciels autorisés propre à chaque dispositif matériel. Au minimum, les exécutables résidents doivent être bloqués.	Exigence obligatoire	Exigence obligatoire	3
		Intervention liée aux vulnérabilités			
ORR-012	Documentation d'intervention	Le système devrait fournir des messages aux administrateurs du système pour expliquer clairement et simplement comment corriger la vulnérabilité.	Exigence souhaitable	Exigence souhaitable	3
ORR-013	Données de correctifs faisant autorité	Le système doit fournir un processus sécurisé de gestion du système des correctifs qui permet d'identifier et vérifier les correctifs pour tous les produits et les systèmes (commerciaux ou gouvernementaux).	Exigence obligatoire	Exigence obligatoire	3
ORR-014	Intervention liée aux vulnérabilités	Le système doit identifier et recueillir des renseignements sur les vulnérabilités, y compris la première fois où elles sont détectées et la première fois qu'elles sont corrigées, sur tous les appareils du réseau, selon un calendrier établi, en fonction des événements et de façon ponctuelle, tel que spécifié par les utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	3
		Intervention relative aux privilèges administratifs			
ORR-015	Intervention relative au niveau de confiance de l'utilisateur	Le système doit appliquer l'accès en utilisant les attributs d'autorisation de niveau de confiance clé disponibles.	Exigence obligatoire	Exigence obligatoire	3
ORR-016	Intervention relative à l'instruction des utilisateurs	Le système doit assurer l'accès des utilisateurs à une installation ou à un compte dans un système en fonction des principales exigences d'autorisation d'instruction.	Exigence obligatoire	Exigence obligatoire	3
ORR-017	Intervention relative aux lacunes en matière de comportement	Le système doit utiliser des vérifications de sécurité automatisées pour fournir la base permettant de corriger automatiquement les lacunes en matière de comportement liées à la sécurité dans le cyberenvironnement du MDN et des FAC.	Exigence souhaitable	Exigence souhaitable	3
ORR-018	Intervention relative aux justificatifs d'identité des utilisateurs	Le système doit assurer l'accès des utilisateurs à une installation ou à un compte dans un système fondé sur les principales exigences d'autorisation des justificatifs d'identité.	Exigence obligatoire	Exigence obligatoire	3
		Intervention relative aux fichiers			
ORR-019	Intervention relative au contrôle des documents	Le système doit appliquer l'utilisation de l'étiquetage des données du MDN et des FAC sur des types de fichiers précis pour appuyer l'inventaire des fonds de données.	Exigence obligatoire	Exigence obligatoire	3
ORR-020	Intervention relative à la sécurité des fichiers	Le système doit protéger la confidentialité, l'intégrité et l'authenticité des données inactives, en transit ou en cours de traitement par cryptographie.	Exigence obligatoire	Exigence obligatoire	3

		Intervention relative aux activités anormales			
ORR-021	Intervention relative au point d'extrémité	Le système doit fournir une capacité de détection et d'intervention des points d'extrémités (IPE) pour intervenir relativement à l'installation de logiciels malveillants sous forme de MPA sur un dispositif de point d'extrémité.	Exigence obligatoire	Exigence obligatoire	3

8.5. Exigences opérationnelles évolutives

Ce tableau comprend les exigences relatives au maintien et à l'amélioration des capacités globales de sécurité et de défense fournies par ce projet aux niveaux de rendement mis en œuvre à la COT.

Les exigences sont ensuite regroupées dans les sous-catégories suivantes :

4. *Soutien en service*. Exigences générales concernant le maintien en puissance des capacités du projet après la mise en œuvre.
5. *Disponibilité*. Exigences concernant l'accès ininterrompu aux capacités opérationnelles.
6. *Distribution des capacités*. Exigences relatives aux configurations globales des capacités.
7. *Extensibilité*. Exigences relatives aux capacités.
8. *Souplesse*. Exigences relatives à la capacité opérationnelle d'accroître et de reconfigurer les capacités.
9. *Développement des capacités*. Exigences relatives à l'amélioration des pratiques exemplaires.
10. *Instruction*. Exigence concernant le perfectionnement des compétences.
11. *Acquisition de changements*. Exigences relatives à l'acquisition de capacités personnalisées et commerciales.
12. *Mise à l'essai des modifications*. Exigences pour vérifier la conformité des capacités aux exigences avant la mise en œuvre.
13. *Mise en œuvre des modifications*. Exigences relatives à la mise en œuvre des capacités dans les opérations.
14. *Résilience*. Exigences relatives au rétablissement des capacités, de la perturbation aux opérations.

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
		Soutien en service			
OER-001	Durée de vie de la capacité	La capacité doit demeurer efficace, adaptative et en service tout au long de son cycle de vie de 10 ans.	Exigence obligatoire	Exigence obligatoire	7.9
		Disponibilité			
OER-002	Type de sites	Le système doit soutenir de façon fiable les sites disponibles et contestés.	Exigence obligatoire	Exigence obligatoire	7.9
		Distribution de la capacité			
OER-006	Traitement central	Le système doit permettre de surveiller, d'analyser, de décider et de réagir de façon centralisée aux conditions de l'infrastructure de TI.	Exigence obligatoire	Exigence obligatoire	7.9

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OER-007	Organisation du traitement centralisé	Le composant de base du système doit être installé de façon centralisée au Centre des opérations du réseau des Forces armées canadiennes (CORFC) à Ottawa en Ontario.	Exigence obligatoire	Exigence obligatoire	7.9
OER-008	Distribution de la propriété	Le système doit maximiser la fonctionnalité et le rendement en utilisant des emplacements qui sont gérés par le MDN, les FAC ou des tiers, ou aux endroits où la gestion est partagée.	Exigence obligatoire	Exigence obligatoire	7.9
OER-009	Capacité de déploiement	Les composants déployables du système doivent être livrés, entrés dans l'inventaire du MDN et des FAC et prêts au déploiement selon les besoins.	Exigence obligatoire	Exigence obligatoire	7.9
		Extensibilité			
OER-010	Extensibilité	Pour répondre au besoin d'évolution, le système doit appliquer les pratiques exemplaires et les lignes directrices de l'industrie afin de s'assurer que le logiciel et le système de la capacité sont : Extensibles – L'ajout d'utilisateurs et/ou de points d'extrémités ne doit pas entraîner une dégradation inacceptable du rendement.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-011	Capacité du site	Le système doit prendre en charge des sites de capacité élevée, moyenne et petite.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-012	Impact sur la capacité	Le système doit réduire au minimum l'utilisation de la bande passante du réseau et des ressources du système de points d'extrémités afin de limiter les répercussions possibles sur les activités opérationnelles et de mission.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-013	Capacité de données	Le système doit stocker, traiter et fournir des données pour les grandes organisations fédérales (en utilisant le seuil d'un million d'appareils) tout en maintenant la rapidité, l'exhaustivité et l'exactitude adéquates des capacités applicables.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-014	Capacité temporaire	Le système doit permettre d'accroître temporairement les capacités informatiques, de réseau et/ou de stockage afin de répondre aux besoins de pointe sans que cela nuise au reste de l'infrastructure.	Exigence obligatoire	Exigence obligatoire	7,8,9
		Flexibilité			
OER-015	Extensibilité	Pour répondre au besoin d'évolution, le système doit appliquer les pratiques exemplaires et les lignes directrices de l'industrie afin de s'assurer que le logiciel et le système de la capacité sont : Extensible – L'intégration de fonctionnalités supplémentaires ne doit pas nécessiter de changements majeurs à l'architecture de la solution existante ou de ses composants/sous-composants individuels.	Exigence obligatoire	Exigence obligatoire	7,8,9

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OER-016	Adaptabilité	Pour répondre au besoin d'évolution, le système doit appliquer les pratiques exemplaires et les lignes directrices de l'industrie afin de s'assurer que le logiciel et le système de la capacité sont : Adaptables et modifiables – Les modifications apportées aux fonctionnalités existantes ne doivent pas nécessiter de modifications majeures à l'architecture de la solution existante ou de ses composants ou sous-composants individuels.	Exigence obligatoire	Exigence obligatoire	7,8,9
		Développement des capacités			
OER-017	Fonctions de développement des capacités	Le MODC doit former les utilisateurs à la fonctionnalité du système grâce à la formation initiale, à la formation continue, au perfectionnement professionnel, au mentorat et à l'encadrement.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-018	Soutien au développement des capacités	Les équipes du MODC doivent soutenir les opérations de cybersécurité.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-019	Structure du développement des capacités	La capacité doit fournir des services professionnels au MDN et aux FAC sous la forme des équipes du MODC pour encadrer, enseigner et encadrer les cyberopérateurs de tous les grades concernés.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-020	Capacité Lieu de développement	La capacité du MODC doit former les utilisateurs pour qu'ils puissent opérer partout où des cyberopérations ont lieu, comme les centres des opérations de cybersécurité et les missions déployées.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-021	Colocalisation du développement des capacités	Les équipes du MODC seront regroupées avec la capacité fournie pendant la mise en œuvre et tout au long de son cycle de vie.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-022	Niveau du développement des capacités	Les équipes du MODC doivent guider les cyberopérateurs à tous les niveaux pour améliorer leurs compétences et améliorer les cyberopérations des FAC afin d'assurer le maintien des compétences.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-023	Maturité du développement des capacités	Les équipes de MODC doivent soutenir la transformation opérationnelle des capacités livrées pour atteindre la capacité d'opérations de sécurité de niveau 5 du NIST.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-024	Environnement de développement des capacités	La capacité de MODC doit former les utilisateurs à exécuter des capacités dans des environnements nationaux, internationaux, centralisés et déployés.	Exigence obligatoire	Exigence obligatoire	7,8,9

		Instruction			
OER-025	Portée de l'instruction	Le système doit fournir une capacité d'instruction pour saisir les pratiques exemplaires et tirer des leçons des opérations précédentes.	Exigence obligatoire	Exigence obligatoire	7.9
OER-026	Capacité de simulation d'instruction	Le système doit dispenser une capacité de simulation d'instruction pour appuyer l'instruction opérationnelle collective dans un contexte opérationnel personnalisable.	Exigence obligatoire	Exigence obligatoire	7.9
OER-027	Portée de la simulation d'instruction	Les scénarios pour les simulations de formation doivent être créés, maintenus, modifiés et exécutés par les cyberopérateurs à partir des systèmes et des postes de travail actuels dans un environnement de formation ou d'exercice.	Exigence obligatoire	Exigence obligatoire	7.9
		Acquisition des modifications			
OER-028	Pratiques des logiciels en développement	Tout logiciel en développement doit être élaboré à l'aide des pratiques exemplaires de l'industrie.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-029	Information sur la menace au développement	Le système doit recueillir et communiquer l'information relative à la mise en œuvre des menaces à la modélisation des systèmes d'information, y compris l'identification des vulnérabilités et des contre-mesures correspondantes.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-030	Information sur la sécurité du développement	Le système doit recueillir et communiquer l'information relative à la mise en œuvre de méthodes de développement de systèmes d'information sécurisés et appliquer des politiques de développement de systèmes d'information sécurisés.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-031	Information sur la sécurité des déploiements de développement	Le système doit recueillir et communiquer l'information relative à la mise en œuvre des méthodes de déploiement des systèmes d'information sécurisés et appliquer les politiques de déploiement des systèmes d'information sécurisés.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-032	Vulnérabilité des politiques de développement	Le système devrait identifier les règlements pertinents, les processus de gouvernance, les politiques de conformité et les CONOPS de sécurité que les acteurs malveillants pourraient exercer pour compromettre les renseignements et le système d'information et effectuer une évaluation des risques pour évaluer l'incidence sur les renseignements et le système d'information.	Exigence souhaitable	Exigence souhaitable	7,8,9
OER-033	Atténuation de la vulnérabilité au développement	Le système devrait mettre en œuvre des méthodes pour minimiser les vulnérabilités ou les faiblesses pendant les activités de conception du système d'information.	Exigence souhaitable	Exigence souhaitable	7,8,9
OER-034	Sécurité du codage au développement	Le système devrait mettre en œuvre des pratiques de codage sécurisé (y compris le codage à sécurité intégrée, le code critique et la protection des données, et la réutilisation des codes sécurisés) pendant le développement du système d'information.	Exigence souhaitable	Exigence souhaitable	7,8,9
OER-035	Acquisition et aliénation des composantes de développement	Le système devrait effectuer l'acquisition sécurisée (p. ex., vérifier la chaîne d'approvisionnement, la chaîne de possession) et l'élimination des composantes et des données dans le cadre du déploiement du système d'information.	Exigence souhaitable	Exigence souhaitable	7,8,9

OER-036	GRCA des composantes du développement	Le système devrait suivre les politiques et les procédures de gestion des risques de la chaîne d'approvisionnement pour établir des bases de référence, faire le suivi et vérifier la provenance des composants du système d'information (pour inclure l'atténuation des contrefaçons, la notation de la réputation et la chaîne de possession) pour l'acquisition ou le développement du système d'information.	Exigence souhaitable	Exigence souhaitable	7,8,9
OER-037	Intégration de la GRCA du développement	La GRCA devrait faire partie intégrante du processus global de gestion des risques et comprendre des directives sur l'évaluation des risques et l'utilisation de contrôles liés à la sécurité pour atténuer les risques cernés.	Exigence souhaitable	Exigence souhaitable	7,8,9
OER-038	Risques liés à la distribution des composantes de développement	La GRCA devrait établir un processus pour déterminer, prévenir, évaluer, signaler et atténuer les risques associés à la nature globale et répartie des chaînes d'approvisionnement de produits et de services de CD-DAR. La gamme des contre-mesures sélectionnées devrait inclure des stratégies appropriées de réduction des risques et la meilleure façon de les mettre en œuvre.	Exigence souhaitable	Exigence souhaitable	7,8,9
		Mise à l'essai des modifications			
OER-039	Objet de l'évaluation des capacités	Le Centre d'évaluation des capacités cybernétiques (CCAEF) doit effectuer des recherches, faire des exercices, mettre à l'essai et évaluer de nouvelles pratiques et solutions en matière de cyberdéfense et de sécurité dans un environnement simulé.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-040	Portée de l'évaluation des capacités	Le CCAEF doit simuler la fonctionnalité et le rendement de tous les domaines cybernétiques du MDN et des FAC ainsi que les mises en garde dans le cadre du projet.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-041	Réseau de l'évaluation des capacités	Le CCAEF doit fournir une représentation de base de la configuration gérée pour chaque facette de tous les domaines cybernétiques du MDN et des FAC et des mises en garde dans le cadre du projet.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-042	Rendement de l'évaluation des capacités	Le CCAEF doit fournir des évaluations fonctionnelles et du rendement du nouveau matériel et des nouveaux logiciels.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-043	Configurations de l'évaluation des capacités	Le CCAEF doit apporter des modifications à la configuration du matériel ou des logiciels installés.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-044	Utilisateurs de l'évaluation des capacités	Le CCAEF doit fournir des ajouts ou des changements à la nature et au nombre d'utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-045	Emplacements de l'évaluation des capacités	Le CCAEF doit fournir des ajouts ou des changements aux points de présence et à leur emplacement.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-046	Effets de l'évaluation des capacités	Le CCAEF doit fournir les effets sur le débit de données et/ou la largeur de bande à n'importe quel point des réseaux.	Exigence obligatoire	Exigence obligatoire	7,8,9

OER-047	Données de l'évaluation des capacités	Le CCAEF doit fournir la collecte des données du journal du système et des données du GIES.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-048	Intégration de l'évaluation des capacités	Le CCAEF doit s'intégrer aux systèmes existants ou prévus d'essai et d'évaluation de l'infrastructure des technologies de l'information.	Exigence obligatoire	Exigence obligatoire	7,8,9
		Mise en œuvre des modifications			
OER-049	Objet des modifications proposées	Le système doit offrir un processus et des outils automatisés pour analyser l'impact que pourraient avoir les modifications proposées au cyberespace pour tous les domaines cybernétiques du MDN et des FAC, à l'exception des modifications proposées.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-050	Portée des modifications proposées	Le système doit fournir un moyen automatisé de faire rapport sur l'incidence des modifications proposées au cyberespace pour tous les scénarios du domaine cybernétique, à l'exception des modifications proposées.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-051	Politique des modifications proposées	Les modifications proposées doivent inclure des modifications à la politique de sécurité, y compris celles qui sont nécessaires pour satisfaire aux exigences du projet.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-052	Conditions des modifications proposées	Le système doit inclure un moyen d'intervention aux menaces et l'ajout, la mise à jour ou la suppression de logiciel, de matériel de configuration ou de conception.	Exigence obligatoire	Exigence obligatoire	7,8,9
OER-053	Processus des modifications proposées	Le système doit traiter toutes les mises à jour de la demande de changement (DDC) et de la gestion de la configuration.	Exigence obligatoire	Exigence obligatoire	7,8,9
		Résilience			
OER-054	Réduction au minimum des perturbations	Le système doit utiliser des caractéristiques qui réduisent au minimum l'interruption de son fonctionnement.	Exigence obligatoire	Exigence obligatoire	7.9
OER-055	Déploiement des environnements débranchés, intermittents et limités	Le système doit offrir un moyen de faire une évaluation rapidement déployable et locale pour appuyer les environnements (p. ex : navires, aéronefs, déploiement en milieu inhospitalier).	Exigence obligatoire	Exigence obligatoire	7.9
OER-056	Rétablissement des environnements débranchés, intermittents et limités	Le système doit fournir une capacité d'évaluation centralisée dans les environnements débranchés, intermittents et limités.	Exigence obligatoire	Exigence obligatoire	7.9
OER-057	Limites de bande passante des environnements débranchés, intermittents et limités	Le système doit fonctionner dans des environnements débranchés, intermittents et limités.	Exigence obligatoire	Exigence obligatoire	7.9

OER-058	Voie alternative des environnements débranchés, intermittents et limités	Le système doit fournir une autre méthode de transfert d'information pour faciliter les environnements débranchés, intermittents et limités.	Exigence obligatoire	Exigence obligatoire	7.9
OER-059	Voie alternative des environnements débranchés, intermittents et limités	Le système doit intégrer l'information recueillie localement lorsque le fonctionnement normal est rétabli, sans compromettre l'information.	Exigence obligatoire	Exigence obligatoire	7.9
OER-060	Sauvegarde des données	Le système doit comprendre des capacités de sauvegarde des données stockées sur le réseau.	Exigence obligatoire	Exigence obligatoire	7.9
OER-061	Interruptions imprévues	Les interruptions imprévues doivent être d'une durée relativement courte (le délai qu'il ne faut pas dépassé doit être défini).	Exigence souhaitable	Exigence obligatoire	7.9
OER-064	Principe de rétablissement	Le système doit être conçu de manière à ce que chaque équipement puisse être réparé, entretenu et remplacé avec un impact minimal sur le fonctionnement de la capacité.	Exigence obligatoire	Exigence obligatoire	7.9
OER-065	Temps de réparation	Le système doit être réparé, entretenu, remplacé et fonctionner en temps opportun conformément à l'énoncé de sensibilité et au processus d'évaluation de la sécurité et d'autorisation.	Exigence obligatoire	Exigence obligatoire	7.9

8.6. Exigences relatives aux tâches opérationnelles

Ce tableau comprend les exigences relatives à la prestation au niveau opérationnel des capacités de CD-DAR aux intervenants sous forme de tâches et de flux de travail.

Les exigences sont ensuite regroupées dans les sous-catégories suivantes :

15. *Interface utilisateur*. Exigences visant à rendre les capacités accessibles aux intervenants.
16. *Tâches*. Exigences visant à rendre les capacités à la disposition des intervenants.

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
		Interface utilisateur			
OTR-001	Capacité de l'interface utilisateur	Le système doit fournir une interface utilisateur intégrée pour accéder à la fonctionnalité qu'offre la solution CD-DAR.	Exigence obligatoire	Exigence obligatoire	4
OTR-002	Principe d'activation de l'interface	Les fonctions automatisées fournies par le système doivent être activées par les utilisateurs et, dans la mesure du possible, par le système.	Exigence obligatoire	Exigence obligatoire	4

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OTR-003	Configurabilité de l'interface axée sur les rôles	Le système doit offrir une interface configurable conviviale appropriée au rôle, aux fonctions et aux tâches de l'utilisateur.	Exigence obligatoire	Exigence obligatoire	4
OTR-004	Interface optimisée de l'utilisateur	Le système doit optimiser l'utilisation du temps du cyberopérateur.	Exigence obligatoire	Exigence obligatoire	4
OTR-005	Accès utilisateur de la RCN	Le système devrait prendre en charge et donner accès à tous les utilisateurs (commandants, cyberopérateurs et personnel de soutien) travaillant ensemble dans les lieux de services de TI de la région de la capitale nationale (RCN).	Exigence obligatoire	Exigence obligatoire	4
OTR-006	Accès des utilisateurs du MDN et des FAC et de SPC	Le système devrait prendre en charge et donner accès à tous les utilisateurs (commandants, cyberopérateurs et personnel de soutien) travaillant ensemble dans les lieux du MDN et des FAC et de SPC.	Exigence souhaitable	Exigence souhaitable	4
OTR-007	Accès des utilisateurs à l'intérieur du Canada	Le système devrait prendre en charge et donner accès à tous les utilisateurs (autorités opérationnelles, cyberopérateurs, gestionnaires, cadres supérieurs et personnel de soutien) travaillant ensemble dans une zone géographique ou un endroit de service situé à l'extérieur de la RCN, mais à l'intérieur du Canada.	Exigence souhaitable	Exigence obligatoire	4
OTR-008	Accès des utilisateurs désavantagés	Le système devrait prendre en charge et donner accès à tous les utilisateurs (autorités opérationnelles, cyberopérateurs, gestionnaires, cadres supérieurs et personnel de soutien) travaillant ensemble dans une zone géographique ou un endroit de service situé à l'intérieur de la RCN, mais déployés à l'étranger dans un endroit de service défavorisé avec des capacités de bande passante limitées.	Exigence souhaitable	Exigence obligatoire	4
OTR-009	Interface Web	Le système devrait être livré dans une application Web.	Exigence souhaitable	Exigence souhaitable	4
		Attribution des tâches			
		Tâche commune			
OTR-010	Capacité de gestion des tâches	Le système doit fournir une capacité de gestion des tâches accessible aux utilisateurs qui identifie, définit et automatise les tâches, les processus et les flux de travail pour exécuter toutes les fonctions de CD-DAR.	Exigence obligatoire	Exigence obligatoire	4
OTR-011	Flux des travaux des incidents liés à la tâche	L'utilisateur doit avoir un flux des travaux d'intervention en cas d'incident automatisé.	Exigence obligatoire	Exigence obligatoire	4
OTR-012	Gestion des tâches d'entreprise	Le système doit fournir une base de données unifiée sur la gestion des tâches qui établit un lien entre les participants aux tâches, les capacités, le calendrier, l'affectation et les données sur les activités.	Exigence obligatoire	Exigence obligatoire	4

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OTR-013	Notes sur les tâches	Le système doit permettre de saisir et de tenir à jour des notes pour tous les types de renseignements afin de traiter du contenu non standard.	Exigence obligatoire	Exigence obligatoire	4
OTR-014	Méthodes de saisie des tâches	Le système doit permettre l'entrée manuelle et par lots de l'information.	Exigence obligatoire	Exigence obligatoire	4
OTR-015	Interopérabilité des tâches	Le système doit permettre l'échange de données avec d'autres systèmes connexes (p. ex., systèmes de billetterie, systèmes de soumission).	Exigence obligatoire	Exigence obligatoire	4
OTR-016	Participants à la tâche	Le système doit identifier de façon unique et relier les rôles, les organisations, les unités organisationnelles, les équipes, les postes organisationnels, les personnes et les autres participants à la capacité d'attribution des tâches.	Exigence obligatoire	Exigence obligatoire	4
OTR-017	Détails des participants à la tâche	Le système doit comprendre des données supplémentaires sur les participants, comme les identificateurs uniques, les titres, la structure hiérarchique et d'autres liens, la classification et d'autres codes, les participants permanents et temporaires, ainsi que les compétences requises, les profils et les modèles.	Exigence obligatoire	Exigence obligatoire	4
OTR-018	Fonctions des participants à la tâche	Le système doit permettre la recherche, la sélection, l'ouverture, la copie des attributs d'un autre utilisateur, la modification et la fermeture de membres subalternes par des utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-019	Disponibilité des participants à la tâche	Le système doit permettre l'ajout et la suppression de la disponibilité des membres subalternes par les utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-020	Préférences des participants à la tâche	Le système doit pouvoir réinitialiser les préférences par rapport aux valeurs par défaut du système par les utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-021	Détails du travail des participants à la tâche	Le système doit pouvoir ajouter, modifier et supprimer les détails du travail des membres (ensembles de compétences, capacité, disponibilité) par les utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-022	Ajustements de la charge de travail des participants à la tâche	Le système doit permettre d'ajuster les charges de travail en fonction de l'évolution des circonstances.	Exigence obligatoire	Exigence obligatoire	4
OTR-023	Problèmes liés à la charge de travail des participants à la tâche	Le système devrait automatiquement fournir des alertes et des avertissements concernant les problèmes d'analyste ou de charge de travail.	Exigence souhaitable	Exigence souhaitable	4
OTR-024	Perfectionnement des compétences des participants à la tâche	Le système devrait mettre en œuvre un encadrement ou une instruction au besoin pour régler les problèmes de charge de travail.	Exigence souhaitable	Exigence souhaitable	4
OTR-025	Fonctions de l'équipe des participants à la tâche	Le système doit pouvoir créer, déplacer, fusionner et supprimer des équipes par des utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OTR-026	Composition de l'équipe des participants à la tâche	Le système doit pouvoir ajouter et retirer des membres d'une équipe par des utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-027	Capacités liées aux tâches	Le système doit définir le type de travail qui fait autorité et qui peut être effectué par les participants et les conditions dans lesquelles le travail est effectué.	Exigence obligatoire	Exigence obligatoire	4
OTR-028	Détails de la capacité de la tâche	Le système doit comprendre des données supplémentaires sur la capacité d'attribution des tâches, comme les responsabilités, les droits (identité, authentification et autorisation), les préférences (langue, accessibilité, canaux privilégiés et valeurs par défaut de l'application), les affectations. (travail, non relié au travail, règles d'affectation), distribution (multisite, multipartenaires), canaux (immédiat, différé, rotation unique) compétences (activités, niveau de compétence et capacité) et disponibilité (calendrier, heures et quarts).	Exigence obligatoire	Exigence obligatoire	4
OTR-029	Activités de la tâche	Le système définira de façon unique toute interaction réelle qui fait autorité entre les participants, son contenu, sa relation avec d'autres interactions (demandes, communications, affectations, problèmes, incidents, problèmes, solutions de rechange et ordres) et renvois aux systèmes et processus connexes (p. ex., demandes de partenaires, billets, services, problèmes, incidents, solutions de rechange).	Exigence obligatoire	Exigence obligatoire	4
OTR-030	Détails de l'activité de la tâche	Le système doit comprendre des données supplémentaires sur l'activité, comme l'état, les participants, les services demandés, l'identification, la description, la classification, l'établissement des priorités, la raison de l'affectation, le moment, la relation avec d'autres demandes et les systèmes partenaires.	Exigence obligatoire	Exigence obligatoire	4
OTR-031	Calendrier des tâches	Le système doit comprendre des données à l'appui du calendrier ciblé et réel des tâches.	Exigence obligatoire	Exigence obligatoire	4
OTR-032	Détails sur le calendrier des tâches	Le système doit comprendre des données additionnelles sur le calendrier, comme l'heure et les dates de début prévues et réelles, l'heure et les dates de fin, l'heure et les dates de notification et les durées.	Exigence obligatoire	Exigence obligatoire	4
OTR-033	Alertes de tâches	Le système doit avoir les capacités d'assignation automatisée et de flux des travaux pour intervenir en cas d'alertes ou de déclenchement.	Exigence obligatoire	Exigence obligatoire	4
		Réception des tâches			
OTR-034	Contexte de réception des tâches	Le système doit établir des liens entre les tâches pour définir le contexte (p. ex., par symptôme, cause fondamentale, intervention, participants, autres systèmes).	Exigence obligatoire	Exigence obligatoire	4
OTR-035	Interopérabilité de l'identification de réception des tâches	Le système devrait permettre l'accès à la solution de gestion d'identification pour confirmer l'admissibilité.	Exigence souhaitable	Exigence souhaitable	4

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
		Analyse des tâches			
OTR-036	Tâches d'analyses répétitives	Le système doit automatiser les tâches d'analyses répétitives.	Exigence obligatoire	Exigence obligatoire	4
OTR-037	Interopérabilité de l'analyse des tâches	Le système devrait permettre l'interopérabilité avec les systèmes de connaissances utilisés par les fournisseurs pour analyser et résoudre les activités.	Exigence souhaitable	Exigence souhaitable	4
		Attribution des tâches			
OTR-038	Fonctions d'attribution de tâche	Le système doit pouvoir visualiser, supprimer, terminer, réactiver et réaffecter les activités des utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-039	Conditions des fonctions des tâches	Le système doit limiter les réaffectations, les suppressions et les complétions aux activités ouvertes; les réactivations aux activités fermées par les utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-040	Automatisation des attributions de tâche	Le système doit automatiser au maximum les affectations au moyen d'un moteur d'affectation alimenté par les données sur les participants et les capacités.	Exigence obligatoire	Exigence obligatoire	4
OTR-041	Ressourcement des attributions de tâche	Le système doit parcourir la structure du participant conformément à la logique d'affectation pour trouver les ressources les plus appropriées pour exécuter et terminer le travail.	Exigence souhaitable	Exigence souhaitable	4
OTR-042	Stratégies des attributions de tâche	Le système doit soutenir diverses stratégies d'affectation (p. ex., selon la topologie des participants, les compétences requises, la disponibilité des ressources, les voies, la priorité, le calendrier).	Exigence souhaitable	Exigence souhaitable	4
OTR-043	Affectations de tâches multiples	Le système doit prendre en charge de multiples affectations.	Exigence souhaitable	Exigence souhaitable	4
OTR-044	Interopérabilité de la logique de l'attribution des tâches	Le système devrait permettre l'accès à d'autres systèmes qui appuient la logique d'affectation.	Exigence souhaitable	Exigence souhaitable	4
OTR-045	Annulation des attributions de tâche	Le système doit permettre d'outrepasser manuellement les attributions de tâche.	Exigence souhaitable	Exigence souhaitable	4
OTR-046	Priorisation des attributions de tâche	Le système doit être en mesure de créer, d'activer, de désactiver, d'accroître la priorité et de réduire la priorité des règles d'acheminement par les utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-047	Ajustements administratifs des attributions de tâche	Le système doit permettre des modifications temporaires à la logique d'affectation pour répondre aux exigences administratives à court terme (p. ex., réaffectations de personnel, défaillances de l'infrastructure locale).	Exigence obligatoire	Exigence obligatoire	4
OTR-048	Options de réaffectation des tâches	Le système doit permettre diverses options de réaffectation, comme le membre spécifié (par liste déroulante, par recherche partielle de nom), le prochain membre disponible, lui-même, les caractéristiques du profil (complexité, langue, etc.).	Exigence obligatoire	Exigence obligatoire	4

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OTR-049	Justification de réaffectation des tâches	Le système doit nécessiter une raison pour effectuer une réaffectation.	Exigence obligatoire	Exigence obligatoire	4
OTR-050	Suivi des attributions de tâche	Le système doit faire le suivi de l'attribution des tâches en fonction de la nature du travail et de la disponibilité des ressources qualifiées pour le faire.	Exigence obligatoire	Exigence obligatoire	4
OTR-051	Événement des attributions de tâche	Le système enregistre et relie toutes les affectations, tous les événements et tous les états dans la base de données des activités pour une visualisation unifiée.	Exigence obligatoire	Exigence obligatoire	4
OTR-052	Avis des attributions de tâche	Le système doit fournir des avis concernant l'état d'avancement des tâches, en particulier les alertes et les avertissements qui informent les agents des menaces potentielles ou réelles aux normes de service (p. ex., avertissements de délai pour permettre des ajustements avant les répercussions sur le service; les retards prévus, l'achèvement de la tâche).	Exigence obligatoire	Exigence obligatoire	4
OTR-053	Progrès des tâches	Le système doit être capable de suivre et de surveiller le progrès des tâches du flux de travail.	Exigence obligatoire	Exigence obligatoire	4
OTR-054	Traçabilité des tâches	Le système doit rapporter les progrès et les observations au processus (ou sous-système ou module) d'où la tâche provient.	Exigence obligatoire	Exigence obligatoire	4
		Compte rendu d'exécution des tâches			
OTR-055	Compte rendu d'exécution des tâches	Le système doit permettre de traiter l'information à partir de différents points de vue afin d'appuyer le traitement efficace des données (p. ex., par rôle, par personne, par divers attributs comme le langage, les types).	Exigence obligatoire	Exigence obligatoire	4
OTR-056	Vues du compte rendu d'exécution des tâches	Le système doit permettre de visualiser l'information sur le rendement à partir d'un certain nombre de points de vue (p. ex., membre, activité, état) et de niveaux (agent, équipe) pour déterminer les niveaux de rendement.	Exigence obligatoire	Exigence obligatoire	4
OTR-057	Modes de compte rendu d'exécution des tâches	Le système doit permettre la visualisation et l'impression en ligne de l'information sur le rendement. Les rapports personnalisés et les rapports standard doivent être pris en charge.	Exigence obligatoire	Exigence obligatoire	4
OTR-058	Fonctions des documents de tâche	Le système doit pouvoir visualiser, déplacer, modifier, supprimer et rétablir les documents connexes par les utilisateurs autorisés.	Exigence obligatoire	Exigence obligatoire	4
OTR-059	Requêtes sur le compte rendu d'exécution des tâches	Le système doit être capable de rechercher et de récupérer avec souplesse les activités pertinentes en fonction de divers critères liés à l'activité et à l'affectation. (p. ex., personne, compétence requise, disponibilité, demande, type de travail, rendement, niveau dans la base de données des affectations).	Exigence obligatoire	Exigence obligatoire	4
OTR-060	Critères du compte rendu d'exécution des tâches	Le système doit permettre des recherches de valeurs et de critères multiples.	Exigence obligatoire	Exigence obligatoire	4

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OTR-061	Organisation du compte rendu d'exécution des tâches	Le système doit permettre le tri, le regroupement et le filtrage des résultats de recherche.	Exigence obligatoire	Exigence obligatoire	4

8.7. Exigences en matière d'information opérationnelle

Ce tableau comprend les exigences communes pour traiter l'information requise par la solution CD-DAR.

Les exigences sont ensuite regroupées dans les sous-catégories suivantes :

17. *Données communes*. Exigences relatives à la gestion générale de l'information.
18. *Interopérabilité*. Exigences relatives à la circulation de l'information entre les fonctions et les emplacements.
19. *Rapports*. Exigences concernant la production et l'affichage de l'information aux intervenants.

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
		Données communes			
OIR-001	Gestion des données d'entreprise	Le système doit fournir un dépôt de données unifié qui fait autorité en matière d'entités cybernétiques et de source de données sur les événements pour toutes les données de CD-DAR.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-002	Détails de la gestion des données d'entreprise	Le système doit offrir la collecte continue, la consolidation et la corrélation des renseignements sur la sécurité et des journaux d'événement des ressources en réseau d'un répertoire d'une petite entreprise afin de mettre en contexte et de fournir des métadonnées et des analyses, des manuels d'appui, et des requêtes et des rapports automatisés (prévus et ponctuels).	Exigence obligatoire	Exigence obligatoire	5.6
OIR-003	Identification des données	Le système doit utiliser une convention d'appellation normalisée pour classifier et définir de façon unique toutes les entités cybernétiques.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-004	Détails sur l'identification des actifs de données	Les données sur l'entité du système doivent comprendre au moins le type d'entité, les réseaux, l'entité virtuelle ou physique, les applications ou les logiciels, la configuration, les dispositifs limites, la criticité de l'entité, l'état et l'emplacement logiques et physiques, la zone physique, l'information sur la solution interdomaines, les comptes administratifs et la propriété (voir les annexes 2 et 3 de la DI).	Exigence obligatoire	Exigence obligatoire	5.6

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OIR-005	Exactitude et couverture des données	Le système doit s'assurer que les renseignements sur les attributs associés à un objet sont à jour dans les xx heures et que la couverture de xx % pour tous les objets est assurée.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-006	Méthode de saisie	Le système doit permettre la création manuelle ou par lots de données du MDN et des FAC (p. ex., par l'intégration avec des dépôts externes d'information sur les actifs ou par des règles opérationnelles).	Exigence obligatoire	Exigence obligatoire	5.6
OIR-007	Enregistrement des données	Le système doit produire des registres de données.	Exigence obligatoire	Exigence obligatoire	5.6
		Interopérabilité des données			
OIR-008	Interopérabilité des partenaires	Le système doit fournir des capacités automatisées d'échange de données avec les partenaires.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-009	Interopérabilité commune	Le système doit permettre l'échange et le partage de données entre toutes les capacités de la solution CD-DAR au moyen d'interfaces et/ou d'API standard, de formats standard et de structures de données standard de CD-DAR, y compris celles pour les actifs, les utilisateurs, l'analyse et les limites.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-010	Normes d'échange de renseignements	Le système doit prendre en charge l'échange et le partage de données entre toutes les capacités de CD-DAR et les capacités externes au moyen d'interfaces standard et/ou d'API, de formats standard et de structures de données de CD-DAR standard.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-011	Données sur les postes de travail interdomaines	Le système doit fonctionner dans un environnement SID pour les utilisateurs du MDN et des FAC (p. ex. de multiples domaines de sécurité sur un seul poste de travail).	Exigence obligatoire	Exigence obligatoire	5.6
OIR-012	Données sur les serveurs interdomaines	Le système doit fonctionner dans un environnement SID côté serveur du MDN et des FAC.	Exigence obligatoire	Exigence obligatoire	5.6
		Rapports			
OIR-013	Distribution de génération de rapports	Le système doit fournir une méthode personnalisable pour générer des rapports, visualiser les résultats du rapport et envoyer des rapports.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-014	Formats des cartes d'actifs	Le système doit fournir une carte réseau de toutes les entités de cyberactifs en divers formats, y compris visuels.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-015	Distribution des cartes d'actifs	Le système doit fournir des cartes d'actifs de TI pour les entités responsables des cyberactifs surveillées aux commandants : par courriel, à l'aide d'un outil logiciel approprié ou au moyen d'une méthode adéquate (comprise dans la CGIEB), conformément aux exigences du processus d'évaluation de la sécurité et d'autorisation.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-016	Rapports d'étape Calendrier	Le système doit fournir des rapports d'état cybernétique sur demande ou selon un calendrier prédéfini.	Exigence obligatoire	Exigence obligatoire	5.6

Numéro de l'exigence	Nom de l'exigence	Détails de la demande	Niveau de COI	Niveau de COT	EOHN Nº
OIR-017	Portée des rapports d'état	Le système doit fournir des rapports d'état cybernétique aux commandants pour les entités de cyberactifs surveillées, comme les appels téléphoniques, la messagerie texte SMS, le courrier électronique, au moyen d'un outil logiciel approprié ou d'une méthode appropriée au sein de la CGIEB.	Exigence obligatoire	Exigence obligatoire	5.6
OIR-018	Processus des rapports d'état	Le système doit fournir des rapports d'état cybernétique définis par les commandants et qui doivent être livrés au moyen d'un processus automatisé fondé sur une liste d'abonnés aux avis.	Exigence obligatoire	Exigence obligatoire	5.6

9. RÉFÉRENCES DU PROJET

Adresses URL	Hyperlien	Lien
https://finland.emc.com/collateral/white-papers/rsa-advanced-soc-solution-sans-soc-roadmap-white-paper.pdf	Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, mai 2015, SANS Institute :	R2
https://collaboration-img.forces.mil.ca/sites/DGCyber/D_Cyber_FD/SSO_CRD/Shared Documents/121018-UU-3136-4-PL-CD-DAR-Project Brief Draft V1.2.docx	CD-DAR Project Brief, v1.2, 12 octobre 2018	R3
	Note de doctrine conjointe – Cyberopérations, article 0608, février 2017	R4
http://dgpaapp.forces.gc.ca/fr/politique-defense-canada/docs/rapport-politique-defense-canada.pdf	La politique de défense du Canada : Protection, Sécurité, Engagement	R6
\\dcs-prk-pv02890\imgdiv$\0_DG_C~1\0_DCYB~1\SSO&CR~1\05-PRO~1\000-OP~1\00-BUS~1\CURREN~1	CD-DAR Business Case Analysis (BCA), v1.9	R7
https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/principaux-organismes-charges-securite.html	Principaux organismes chargés de la sécurité	R9
http://collaboration-admpa.forces.mil.ca/sites/DI/Departmental%20management/project-pad.pdf	Directive sur l'approbation des projets, ministère de la Défense nationale, 16 décembre 2014	R12
http://collaboration-admpa.forces.mil.ca/sites/DI/Departmental%20management/project-pad.pdf	Définition du processus d'approbation des projets, MGP 1/13, 13 août 2013	R13
https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html	Plan de gestion des événements de cybersécurité du gouvernement du Canada	R18
https://www.hsdl.org/?view&did=734860	Lexique des cyberopérations du DoD 2010-2011, page 8, section 16	R24

https://pubs.drdc-rddc.gc.ca/BASIS/pcandid/www/frepub/DDW?W%253DSYSNUM=532776	Cyberopérations des FAC dans le concept d'environnement cybernétique futur, RDDC CARO DT 2009-058, décembre 2009, p. 2.	R25
http://publications.gc.ca/collections/collection_2016/scrs-csis/PS73-2-2016-06-03-fra.pdf	SCRS 2018 – Perspectives sécuritaires 2018 : Risques et menaces éventuels, 2016	R26
https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/plans-priorites.html	Rapport sur les plans et les priorités de 2016-2017	R27
http://cid-bic.forces.mil.ca/Cid/Data/Documents/3349/Draft%20Preliminary%20SOR%20-%20ITI%20in%20Sp%20of%20C2,%20v0.1,%2016%20Nov%2018.pdf	Infrastructure de technologie de l'information à l'appui du commandement et du contrôle (ITI à l'appui du C2) EBO préliminaire, 16 novembre 2018	R30
https://buyandsell.gc.ca/cds/public/2017/12/18/637ad14072ef720ed0c51146992cca46/ABES.PROD.PW__QE.B049.E26594.EBSU000.PDF	DDR CD-DAR	R31
https://collaboration-img.forces.mil.ca/sites/DGCyber/D_Cyber_FD/SSO_CRD/Shared%20Documents/161129-UU-3136-1-PJT-DG%20Cyber-CSA%20Project%20Charter-Final_as_signed.docx	Charte du projet de CD-DAR	R32
	Principes et politiques de gestion de projet du MDN, mai 1999;	R34
https://www.canada.ca/fr/secretariat-conseil-tresor/services/gestion-information-technologie-projets/gestion-projects/guide-outils-gestion-analyse-resultat.html	Guide et outils de gestion par analyse de résultat	R37
https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf	Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee	R38
	CONSUP CD-DAR, V1.1	R39

https://www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes/directives-ordonnances-administratives-defense/serie-4000.html	DOAD 4003-0, Protection et gérance de l'environnement	R40
	Gestion de l'interdépendance des projets de CD-DAR	R41

10. GLOSSAIRE

Termes du glossaire	Description du glossaire
Analyse criminalistique	L'analyse criminalistique est un terme d'analyse approfondie, d'enquête dont le but est d'identifier et de documenter objectivement les coupables, les raisons, le cours et les conséquences d'un incident de sécurité ou d'une violation des lois de l'État ou règles de l'organisation.
Apprentissage machine	Processus par lequel une unité fonctionnelle améliore son rendement en acquérant de nouvelles connaissances ou compétences, ou en réorganisant les connaissances ou les compétences existantes. [Source : Banque de terminologie de la Défense, fiche nº 21880]
Attaque des réseaux informatiques	Une opération militaire qui vise à interdire l'accès aux systèmes des technologies de l'information ou à l'information qui y est hébergée ou à perturber, à détériorer ou à détruire cette information ou ces systèmes. [Source : Politique provisoire du MDN et des FC sur les opérations du réseau informatique des FC, 21 novembre 2013]
Autorité opérationnelle	Personne qui a l'autorité de définir des besoins et des principes directeurs, de fixer des normes et d'accepter des risques dans son domaine de responsabilité. [Source : Banque de terminologie de la Défense, fiche nº 43435]
Autorités opérationnelles	Commandants et leurs états-majors (comme le MDN, le CEMD, le cmdt du COIC, le DOS de l'EMIS ainsi que les autres commandants stratégiques et opérationnels et leurs états-majors) qui comptent activement sur les services de TI pour réussir leurs missions, opérations et tâches, qu'il s'agisse de services ou de fonctions administratives d'ordre national, international, expéditionnaire ou ministériel. Il s'agit des consommateurs finaux des produits de connaissance de la situation de la solution de la solution CD-DAR. [Source : Nouvelle définition]
Bibliothèque de l'infrastructure des technologies de l'information	Ensemble de pratiques détaillées en matière de gestion des services de TI [GSTI] visant à aligner les services de TI sur les besoins opérationnels.
Chaîne de cyberdestruction	Collecte des processus liés à l'utilisation de cyberattaques sur les systèmes.
Chaîne de possession numérique	Préservation de l'intégrité de la preuve numérique ainsi que d'une procédure d'exécution de la documentation chronologique vers la preuve.
Connaissance de la situation	Connaissance des éléments de l'environnement opérationnel nécessaire pour prendre des décisions informées. [Source : Banque de terminologie de la Défense, fiche nº 41441]

Termes du glossaire	Description du glossaire
Cyberactif	Dispositifs électroniques programmables et réseaux de communication, y compris le matériel, les logiciels et les données. [Source : North American Electric Reliability Corporation, Glossary of Terms Used in Reliability Standards 14 (25 mai 2012)]
Cyberentité	Une cyberentité est définie comme « toute chose distincte ou tout acteur distinct qui existe dans l'infrastructure cybernétique [cyberespace] ».
Cyberenvironnement (ou Cyberterrain)	Réseau interdépendant de structures de TI, incluant Internet, les réseaux de télécommunications, les systèmes informatiques et les contrôleurs intégrés ainsi que les logiciels et les renseignements qu'ils contiennent. [Source : Introduction aux cyberopérations des FAC, février 2014.]
Cyberespace	Le réseau interdépendant de structures de technologie de l'information, incluant Internet, les réseaux de télécommunications, les systèmes informatiques ainsi que les processeurs et les contrôleurs intégrés, notamment le logiciel et les renseignements qu'ils contiennent. [Source : Note de doctrine conjointe – Cyberopérations v6]
Cybermenace	Une cybermenace est un événement ou un acte délibéré ou accidentel susceptible d'entraîner la compromission d'un système de TI du gouvernement du Canada. [Source : Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC), 4 août 2015 [R18]]
Cyberopération offensive	Cyberopération offensive. Opération offensive ayant pour but de projeter une puissance dans le cyberespace ou au moyen de celui-ci pour produire des effets à l'appui d'objectifs militaires. [Source : Cyberopérations, Note de doctrine interarmées v6; dossier DTB 693752]
Cyberopérations	Les cyberopérations sont définies comme la conduite d'opérations offensives, défensives et de soutien dont le principal but est l'atteinte des objectifs dans le domaine cybernétique ou au moyen du domaine cybernétique. [Source : Note de doctrine conjointe – Cyberopérations v6]
Cyberopérations de soutien	Opération de réseau assignée par un commandant, ou sous son contrôle direct, en soutien de cyberopérations offensives ou défensives. [Source : Compte rendu des décisions – Réunion du Comité mixte de terminologie tenue au Centre de guerre des Forces canadiennes du 26 au 29 avril 2016]

Termes du glossaire	Description du glossaire
Cyberopérations défensives	Cyberopérations défensives. Une opération défensive menée dans le cyberespace ou au moyen du cyberespace pour détecter, vaincre ou atténuer les actions offensives et exploitantes pour maintenir la liberté d'action. [Source : Cyberopérations, Note de doctrine interarmées v6; dossier DTB 693742]
Cybersécurité	Ensemble des technologies, des processus, des pratiques et des mesures d'atténuation et d'intervention conçues pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés afin d'assurer la confidentialité, l'intégrité et la disponibilité. [Source : TERMIUM Plus®, Banque de données terminologiques et linguistiques du gouvernement du Canada, 9 octobre 2014.]
Défense des réseaux informatiques	Mesures visant à protéger, à surveiller, à analyser, à détecter et à aborder les activités non autorisées menées dans les systèmes d'information et des réseaux informatiques. Il s'agit également d'une mesure prise en vue d'assurer une protection aux réseaux de technologie de l'information contre les activités non autorisées, de surveiller les réseaux, d'analyser les activités, de repérer les activités non autorisées, de surveiller ces activités et de les contrer. [Source : Politique provisoire du MDN et des FC sur les opérations du réseau informatique des FC, 21 novembre 2013]
Détection	Découverte par un moyen quelconque de la présence d'une personne, d'un objet ou d'un phénomène susceptible d'avoir un intérêt militaire. Dans un contexte cybernétique, la détection est axée sur les entités cybernétiques et la découverte, la saisie, l'enregistrement, le suivi et la maintenance de leurs attributs clés.
Détruire	Détruire est un verbe utilisé dans le cadre des tâches de mission qui consiste à endommager un objet ou une force ennemie de façon qu'il soit inutilisable à moins d'être remis en état ou reconstitué. Dans un contexte cybernétique, il peut s'agir d'actions offensives contre la confidentialité, l'intégrité ou la disponibilité des données ou de l'information qui sont obligatoires aux opérations ennemies et qui rendent les opérations ennemies inutiles jusqu'à ce qu'elles soient reconstituées. (Par exemple, supprimer tous les fichiers d'un serveur, réécriture des données d'entrée-sortie de base, d'un système ou d'un micrologiciel, ou causer des dommages physiques aux systèmes de contrôle industriel, etc.)

Termes du glossaire	Description du glossaire
Domaine cybernétique	Ensemble des domaines, des entités et des activités liés au cyberespace ou ayant une incidence sur celui-ci. Note de définition : Le domaine cybernétique comprend l'infrastructure dépendante et les personnes ou utilisateurs du cyberespace. [Source : Note de doctrine conjointe – Cyberopérations v6]
Énoncé de sensibilité	Description des exigences relatives à la confidentialité, à l'intégrité ou à la disponibilité qui s'appliquent aux données ou aux autres biens stockés, traités ou transmis par un système d'information. Source : Termium
Entité responsable des actifs	Matériel réel et souhaité, identité du logiciel, configuration, vulnérabilités connues et privilèges administratifs.
Exploitation des réseaux informatiques	Activité de collecte de renseignements ayant pour but d'avoir accès à des données et de les recueillir à partir d'un STI d'un adversaire, d'un adversaire éventuel ou d'une autre partie approuvée par le gouvernement du Canada, ou de contrôler ce STI. [Source : Politique provisoire du MDN et des FC sur les opérations du réseau informatique des FC, 21 novembre 2013]
Gestion de l'information	Discipline qui consiste à orienter et à appuyer la gestion efficace et efficiente de l'information au sein d'une organisation, et ce, du stade de la planification et de l'élaboration des systèmes jusqu'à celui de leur élimination ou de leur conservation à long terme. [Source : Secrétariat du Conseil du Trésor du Canada, Cadre stratégique pour l'information et la technologie, 1er juillet 2007.]
Identification	L'identification est un processus consistant à atteindre une caractérisation précise d'une entité détectée par une action ou un moyen quelconque de manière à pouvoir prendre des décisions en temps réel, y compris l'engagement ESA des armes, avec un niveau de confiance élevé. Dans un contexte cybernétique, cela signifie qu'il faut effectuer l'analyse d'une entité cybernétique de façon suffisamment détaillée et avec une chaîne juridique de preuves pour permettre aux commandants de cyberforces de prendre des décisions opérationnelles et des plans pour prendre des mesures appropriées au besoin. Dans certains cas, cette tâche peut comprendre une analyse criminalistique détaillée des artéfacts matériels et logiciels guidée par une compréhension approfondie des renseignements sur les menaces.
Infrastructure de technologie de l'information	L'ensemble des ordinateurs, des communications, des logiciels d'exploitation, des programmes utilitaires et des outils de gestion qui soutiennent l'automatisation de la gestion de l'information à l'échelle d'une organisation. L'ITI ne comprend pas les applications et leurs bases de données connexes. [Source : Banque de terminologie de la Défense, fiche no 1837]

Termes du glossaire	Description du glossaire
Intelligence artificielle	L'intelligence artificielle (IA) est la simulation de processus d'intelligence humaine par des machines, en particulier des systèmes informatiques. Ces processus comprennent l'apprentissage (l'acquisition d'information et les règles d'utilisation de l'information), le raisonnement (l'utilisation de règles pour arriver à des conclusions approximatives ou définitives) et l'autocorrection.
Lieu de services de technologie de l'information	Poste de travail, bureau, immeuble ou espace similaire dans une zone de prestation de services où les personnes établissent leurs points distincts d'interaction avec la technologie de l'information. [Source : Nouvelle définition pour le projet de CD-DAR]
Mesures d'intervention	En cyberopérations défensives, mesures prises et activités menées dans le cyberespace ou au moyen de celui-ci, à l'extérieur de son propre cyberespace, pour contrer des menaces actuelles ou imminentes en vue de conserver la liberté d'action. [Source : Compte rendu des décisions – Réunion du Comité mixte de terminologie tenue au Centre de guerre des Forces canadiennes du 26 au 29 avril 2016]
Mesures de défense internes	Les mesures de défense internes sont des mesures prises et des activités menées dans son propre cyberespace pour assurer la liberté d'action.
Neutraliser	Neutraliser est un verbe utilisé dans le cadre des tâches de mission qui consiste à rendre temporairement un élément ennemi incapable d'entraver une opération en particulier. La tâche doit indiquer clairement ce qu'il faut neutraliser. Il est ambigu d'énoncer simplement « neutraliser les préparatifs de l'ennemi » ou « neutraliser les forces de sécurité de l'ennemi ». Dans un contexte cybernétique, il peut s'agir d'actions offensives contre la confidentialité, l'intégrité ou la disponibilité des données ou de l'information qui empêchent les unités des forces ennemies d'utiliser leurs cybercapacités offensives ou défensives (par exemple, interrompre les flux de capteurs d'un domaine cible à l'unité de cyberdéfense responsable).
Opérations de réseaux informatiques	Opérations comprenant les attaques de réseaux informatiques, la défense de réseaux informatiques et l'exploitation de réseaux informatiques. [Source : Politique provisoire du MDN et des FC sur les opérations du réseau informatique des FC, 21 novembre 2013]
Ordinateur hôte	Dans un réseau informatique, un ordinateur qui fournit aux utilisateurs finaux des services comme le calcul et l'accès à la base de données et qui peut exécuter des fonctions de contrôle de réseau [Source : Banque de terminologie de la Défense, fiche nº 13461]

Termes du glossaire	Description du glossaire
Reconnaissance	La reconnaissance signifie la détermination, par quelque moyen que ce soit, du caractère amical ou ennemi ou de l'individualité d'un autre, ou d'objets tels que des aéronefs, des navires, des chars d'assaut ou de phénomènes tels que les modèles de communications électroniques. Dans un contexte cybernétique, cela signifie analyser les attributs clés des entités cybernétiques et de leurs activités (sur la conviction que les données sur de nombreux attributs peuvent être fausses, périmées, incomplètes ou trompeuses, etc.) dans le contexte holistique du domaine des opérations mondiales et interarmées ou de l'information, pour déterminer si les activités observées sont le résultat de menaces naturelles ou délibérées et estimer les répercussions de ces menaces.
Renseignement	Produit de la recherche, du traitement, de l'analyse, de l'intégration et de l'interprétation des informations disponibles sur les États étrangers, les forces ou éléments hostiles ou susceptibles de l'être, la géographie et les facteurs sociaux et culturels qui contribuent à la compréhension de l'environnement opérationnel réel ou potentiel. Remarque : Le terme « renseignement » décrit également les activités qui mènent au produit, ainsi que les organisations qui les exécutent. [Source : Banque de terminologie de la Défense, fiche nº 738]
Renseignement d'origine électromagnétique (SIGINT)	Examen détaillé des données et de l'information de RSI d'une seule discipline du renseignement, mené par des ressources de transformation spécialisées, conformément à l'attribution des tâches de transformation. [Source : Compte rendu des décisions – Réunion du Comité mixte de terminologie tenue au Centre de guerre des Forces canadiennes du 26 au 29 avril 2016]
Réseau de commandement	Réseau de communications qui relie un échelon de commandement à une partie ou à la totalité de ses échelons subalternes aux fins de commandement et de contrôle. L'infrastructure du réseau secret consolidé (IRSC) fait partie du réseau de commandement du MDN et des FAC. Le réseau de commandement comprend les extensions et les interfaces du R comd et les systèmes du RED déployables. Tout au long de ce document, l'expression « réseau de commandement » sera utilisée pour inclure les termes ci-dessus.
Résultat	Un résultat est « tout ce qui arrive à la suite et comme effet de quelque chose ». [Source : Guide et outils de gestion par analyse de résultat [R37]]
Service de technologie de l'information	Points distincts d'interaction entre la technologie de l'information et les personnes, tant à l'intérieur qu'à l'extérieur d'une organisation. [Source : Nouvelle définition pour le projet de CD-DAR]

Termes du glossaire	Description du glossaire
Supprimer	La suppression consiste à dégrader temporairement une capacité de l'ennemi pour permettre une action des forces amies. L'effet est temporaire et il ne dure qu'aussi longtemps que la force amie fait feu. Dans un contexte cybernétique, il peut s'agir d'une série de cyberactions offensives qui dégradent ou neutralisent la capacité d'une force belligérante d'utiliser le cyberespace. (Exemple : Les attaques entraînant un déni de service).
Système d'information	Un ensemble d'équipements, de méthodes et de procédures et, au besoin, de personnel organisé de manière à remplir des fonctions de traitement de l'information. Remarque : Un système d'information peut également assurer le transfert d'informations en plus des fonctions de traitement, par exemple au sein d'un réseau local reliant plusieurs ordinateurs faisant partie du système d'information. [Source : Banque de terminologie de la Défense, fiche n^{o} 20171]
Systèmes des technologies de l'information	Ensemble du matériel informatique, des logiciels ou des micrologiciels, fonctionnant en autonomie ou en réseau, utilisés afin de traiter/transmettre des données ou de contrôler des appareils mécaniques ou d'autres dispositifs. [Source : Banque de terminologie de la Défense, fiche n^{o} 48262]
Technologie de l'information	Matériel ou système utilisé pour l'acquisition, le stockage, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, la commutation, les échanges, la transmission ou la réception automatiques de données ou de renseignements. Elle englobe la conception, le développement, l'installation et la mise en œuvre de systèmes et d'applications informatiques visant à satisfaire à des exigences opérationnelles. [Source : Secrétariat du Conseil du Trésor du Canada, Cadre stratégique pour l'information et la technologie, 1er juillet 2007.]

11. SIGLES, ACRONYMES ET ABRÉVIATIONS

	Description
AAS	Autorisation et accréditation de sécurité
AD – COD	Aide à la décision pour les cyberopérations défensives
ADR	Analyse des décisions et réponse
AF	Année financière
AM	Apprentissage machine
AM	Autres ministères
AN	Approvisionnement national
AO	Autorité opérationnelle
AP (Déf)	Approbation du projet (Définition)
AP (MEO)	Approbation du projet (Mise en œuvre)
AR	Analyse de rentabilisation
ARC	Aviation royale du Canada
BDNV	Base de données nationale sur les vulnérabilités
BGSN	Bureau de gestion des services nationaux
BITI	Bibliothèque de l'infrastructure des technologies de l'information
C Cyber	Chef du personnel du cyberespace
C2	Commandement et contrôle
C4ISR	Commandement, contrôle, informatique, communications, renseignement, surveillance et reconnaissance
CARO	Centre d'analyse et de recherche opérationnelle
CCCFI	Commandant de la composante cybernétique des forces interarmées
CCD	Conseil des capacités de la Défense
CD-DAR	Cyberdéfense – Analyse des décisions et réponse
CDADS	Analyse de la cyberdéfense et prise en charge des décisions
CDR	Dépôt des cyberdonnées
CEED	Cyberentités et découverte d'événements
CEIAD	Commission d'examen indépendante d'acquisition de la Défense
CEMD	Chef d'état-major de la défense
CGIR	Comité de gestion des investissements et des ressources
CGP	Conseil de gestion de programme
CNGS	Centre national de gestion des services
COD	Tableau de bord opérationnel cybernétique

	Description
COD	Cyberopérations défensives
COI	Capacité opérationnelle initiale
COIC	Commandement des opérations interarmées du Canada
COMFOSCAN	Commandement – Forces d'opérations spéciales du Canada
COMM N	Communicateurs navals
CONOPS	Concept des opérations
CONSOUT	Concept de soutien
CORFC	Centre d'opérations des réseaux des Forces canadiennes
COSD	Centre des opérations des services de la Défense
COT	Capacité opérationnelle totale
CS	Connaissance de la situation
CSC	Contrôles de la sécurité critique
CSE	Comité supérieur d'examen
CSMA	Surveillance et mesures de cybersécurité
CST	Centre de la sécurité des télécommunications
CYBEROP	Cyberopérateur
D Sécur GI	Directeur – Sécurité (Gestion de l'information)
DAP	Directive d'approbation de projet
DAT	Document d'architecture technique
DDP	Demande de propositions
DG Cyberespace	Directeur général – Cyberespace
DGGC	Comité de gouvernance des directeurs généraux
DGOGI	Direction générale – Opérations (Gestion de l'information)
DGRPGI	Directeur général, Réalisation de projets (Gestion de l'information)
DI	Demande d'information
DIL	Déconnecté, intermittent, limité (faible largeur de bande)
DIPE	Détection et intervention aux points d'extrémité
DMR	Durée moyenne des réparations
DoD	Département de la défense des États-Unis
DPC	Dénombrement des plates-formes communes
DPMEF	Directeur – Présentations ministérielles et ententes financières
DR	Bureau de services régional

	Description
DSAMD	Stratégie d'approvisionnement en matière de défense
É.-U.	États-Unis
EBO	Énoncé des besoins opérationnels
EECI	Environnement d'essai cyberintégré
EICC	Équipe d'intervention en cas de catastrophe
EICO	Équipe interarmées des cyberopérations
ÉMIS	État-major interarmées stratégique
EOHN	Exigences obligatoires de haut niveau
EP(ID)	Énoncé de projet (identification)
ESN	Exemption au titre de la sécurité nationale
FAC	Forces armées canadiennes
GC	Gouvernement du Canada
GIES	Gestion de l'information et des événements de sécurité
Gp5	Groupe des cinq
GSTI	Gestion des services de technologie de l'information
GT	Gestion des tâches
IA	Intelligence artificielle
ICSO	Image commune de la situation opérationnelle
IPCP-IA	Analyse de l'incidence des changements apportés au plan d'investissement
IPO	Instruction permanente d'opérations
ITI	Infrastructure de technologie de l'information
ITI à l'appui du C2	Infrastructure de technologie de l'information à l'appui du commandement et du contrôle
Langage KML	Keyhole Markup Language
MDI	Mesures de défense internes
MDN	Ministre de la Défense nationale
MDN et FAC	Ministère de la Défense nationale et Forces armées canadiennes
MODC	Mentorat opérationnel et développement de capacité
MPA	Menaces persistantes avancées
MRC	Marine royale du Canada
MTBF	Moyenne des temps de bon fonctionnement
NGP	Note de service destinée à servir de guide sur le programme
NORAD	Commandement de la défense aérospatiale de l'Amérique du Nord

	Description
NSA	National Security Agency
NS-SCC	Établissement de contrats nécessitant des avertissements de sécurité nationale spéciaux
NVG	NATO Vector Graphics
ONU	Nations Unies
OP EICM	Opérateurs d'équipement d'information de combat (Marine)
OREN	Objectif de rendement
OSINT	Renseignement de sources ouvertes
OTAN	Organisation du Traité de l'Atlantique Nord
PA	Plan d'action
PACS	Systèmes de contrôle des accès physiques
PAR	Passerelle d'accès aux réseaux
PCAP	Capture de paquets
PF & E	Personnel, fonctionnement et entretien
PGEC GC	Plan de gestion des événements de cybersécurité du gouvernement du Canada
PI	Protocole Internet
PMOP	Plan de mise en œuvre du projet
PPER	Possibilités du projet et évaluation des risques
PSE	Protection, Sécurité, Engagement
Qté	Quantité
R comd	Réseau de commandement
RA	Mesures d'intervention
RCN	Région de la capitale nationale
RDDC	Recherche et développement pour la Défense Canada
RED	Réseau étendu de la Défense
RT	Responsable technique
RU	Royaume-Uni
SCS	Sensibilisation à la cybersécurité
SCT	Secrétariat du Conseil du Trésor
SDI	Système de détection des intrusions
SDI	Système de détection d'intrusion
SEO	Système d'entraînement opérationnel
SES	Soutien en service
SIGINT	Renseignement d'origine électromagnétique

	Description
SMA(GI)	Sous-ministre adjoint (Gestion de l'information)
SPAC	Services publics et Approvisionnement Canada
SPC	Services partagés Canada
STI	Système de technologie de l'information
SVRS	SysAdmin, Vérification, Réseau et Sécurité
TI	Technologie de l'information
TVH	Taxe de vente harmonisée
UC	Unité centrale de traitement
VEF	Vulnérabilités et expositions fréquentes
Zresp	Zone de responsabilité

ANNEXE A – DESCRIPTION DES COMPOSANTS FONCTIONNELS CYBERNÉTIQUES

Id	Composant	Description
1	Tableau de bord opérationnel cybernétique	Visualisation et production de rapports Le COD offre plusieurs tableaux de bord, vues dynamiques et des fonctions de rapports afin d'appuyer toutes les utilisations nécessaires aux utilisateurs concernés. Le tableau de bord permet aux utilisateurs clés (comme les gestionnaires, les cadres, les analystes, etc.) de voir l'état des cyberentités à partir de leur bureau. Le COD peut présenter différents types d'affichages selon les exigences configurables de l'utilisateur. Les affichages peuvent être textuels, une liste de table textuelle, des graphiques à barres, des graphiques de tendance, une carte géographique, etc. Interface utilisateur Le terme « tableau de bord » fait référence à un affichage d'information à écran unique utilisé pour faire le suivi de l'état des cyberentités et de leurs comportements. Le COD est l'endroit de travail principal pour tous les cyberopérateurs et les utilisateurs du dépôt des cyberdonnées. C'est par l'entremise du COD que chaque cyberopérateur effectue et gère ses tâches (p. ex. : flux de travail, suivi des événements, bon de travail, analyses, saisie de données dans le CDR, gestion du CDR, etc.). Le COD peut être mis en œuvre comme une interface unique ou un ensemble de différentes applications selon le choix de conception et les contraintes de mise en œuvre. Accès aux données et intégration Le COD est une interface visuelle où tous les utilisateurs humains peuvent accéder aux renseignements conservés dans le dépôt des cyberdonnées afin d'améliorer la connaissance de la situation de la cyberdéfense et d'aider le traitement des incidents. Le COD fournit des flux de données normalisés qui peuvent être utilisés par les capacités existantes de gestion de l'espace de combat et les applications C2, en utilisant des formats de données standards tels que KML (Keyhole Markup Language) et NVG (NATO Vector Graphics), afin de visualiser la situation de la cyberdéfense avec d'autres couches de la situation militaire comme les unités terrestres, aériennes et maritimes. Analyse Le COD contient des outils d'analyse graphique et un accès aux composants des systèmes CEED, CSMA, CDR, CDADS et TM.

Id	Composant	Description
2	Gestion des tâches	Ce composant comprend le système de gestion de l'allocation de tâches, des bons de travail et du flux de travail. Par l'entremise du COD, les cyberopérateurs et les gestionnaires appropriés peuvent utiliser le sous-système de la gestion des tâches pour avoir accès aux services de tâches, de bons et de flux de travail pour contrôler, suivre et gérer les travaux et les priorités des cyberopérateurs. La gestion des tâches permet aux superviseurs de quarts, aux gestionnaires, aux commandants et aux autres cadres de définir les tâches, les priorités de surveillance et les priorités de travaux en plus de réviser l'état des tâches, de gérer les horaires, d'administrer le flux de travail, etc.
3	Entraînement opérationnel	Ce composant d'entraînement est utilisé pour s'assurer que les cyberopérateurs, les gestionnaires, les cadres et les autres opérateurs sont à jour et maîtrisent leurs tâches, rôles et responsabilités dans le système intégré, y compris : a. la capacité de créer une simulation de menace, de pénétration et d'attaque opérationnelle pour exercer l'équipe de cyberopérateurs et évaluer leur état de préparation opérationnelle ainsi que leur efficacité; b. un composant d'entraînement opérationnel individuel axé sur les opérateurs individuels (tâches, rôles, progrès dans leur rôle); c. une instruction axée sur les compétences et la validation des cyberopérateurs, opérateurs et civils dans leur rôle attribué autant au niveau individuel que collectif; d. un composant d'instruction collective pour une capacité d'analyse des décisions et réponse. Ceci est une réplique d'un ensemble de systèmes d'exploitation avec des ensembles de données hors ligne pour permettre une gamme complète de fonctions et de scénarios réalistes à des fins de formation.
4	Surveillance et mesures de cybersécurité	Ce composant surveille continuellement le dépôt des cyberdonnées (CDR) pour identifier la présence de cyberentités non conformes, d'événements, d'alertes, de vulnérabilités ou autres changements à l'état des cyberentités dans le cyberespace du MDN et des FAC. Le système donne l'alerte aux cyberopérateurs adéquats lors de la présence de cyberentités ou comportements non conformes. Le sous-système réagit aussi aux alertes associées à la non-conformité pour donner l'autorisation aux configurations de cybersécurité des cyberentités et pour recommander une intervention corrective automatique (p. ex. : gestion des correctifs, mise à jour du système, jardin fermé, réduction d'utilisateurs ou des privilèges des applications, etc.) ou avec l'intervention d'un cyberopérateur. Ce composant effectue les activités essentielles liées à la sécurité comme la gestion des biens, l'évaluation des vulnérabilités, le contrôle de documents, la gestion de la configuration et les fonctions du changement de configuration telles que l'évaluation de la sécurité et le processus d'autorisation. Cela inclut aussi la mise en œuvre des contrôles de la sécurité critique (CSC) du centre de sécurité Internet (CIS) de 1 à 5 grâce aux interactions avec le CDR. Les éléments essentiels minimaux pour le CSC sont : CSC-1 L'inventaire des appareils autorisés et non autorisés; CSC-2 L'inventaire des logiciels autorisés et non autorisés; CSC-3 La configuration sécuritaire des appareils des utilisateurs finaux; CSC-4 L'évaluation et les mesures correctives continuelles des vulnérabilités; CSC-5 L'utilisation contrôlée des privilèges administratifs.

Id	Composant	Description
5	Analyse de la cyberdéfense et prise en charge des décisions	Ce composant surveille et analyse continuellement les dépôts de cyberdonnées (CDR) pour identifier de possibles vulnérabilités ou des cyberattaques et des intrusions dans le domaine cybernétique du MDN et des FAC. Le système donne l'alerte aux cyberopérateurs adéquats lors de la détection de vulnérabilités, de menaces, de risques ou de comportements. Il s'accorde automatiquement sans cesse pour réduire les faux positifs et les faux négatifs. Le système réagit aussi à toutes les cyberalertes et recommande au cyberopérateur des mesures correctives appropriées et leur impact. Il sera aussi capable d'automatiser l'exécution de mesures d'intervention préapprouvées. Le système permet notamment : a. L'évaluation des facteurs de risque dynamiques (ERD) pour permettre aux intervenants de définir (et maintenir avec le temps) l'importance de leurs objectifs de mission et la dépendance de ceux-ci au cyberespace du MDN et des FAC. La capacité de l'ERD va corréler dynamiquement tous les renseignements fournis par le CDR afin d'évaluer continuellement les risques. La signature de risque sera disponible pour tous les utilisateurs pertinents de l'interface COD. b. La gestion des facteurs de risque dynamiques (DRM) pour appuyer les décideurs avec la gestion des risques qui sont identifiés par l'ERD. À cette fin, la capacité du DRM peut recommander une intervention individuelle ou un plan d'action complet en plus d'évaluer leur efficacité, leurs coûts et les effets secondaires relatifs aux objectifs de la mission. c. Les renseignements cybernétiques et l'analyse d'OSINT. d. La chasse et les analyses avancées; e. L'analyse criminalistique; f. Le traitement des incidents; g. Intervention en cas d'incident avec analyse du plan d'action; h. Le contrôle de la sécurité du réseau et la production de rapports; i. La planification opérationnelle.

Id	Composant	Description
6	Dépôt des cyberdonnées (CDR)	Une banque de données qui agit comme l'entrepôt pour les cyberentités autorisées et les données d'événements pour le cyberespace du MDN et des FAC. Il conserve toutes les données liées à la collection de toutes les cyberentités présentes dans le cyberespace du MDN et des FAC en plus d'une description de la relation entre ces entités en vue d'analyses des liens, d'analyses de vulnérabilités, de détection des intrusions, d'analyses criminalistiques et d'autres tâches relatives à la cybersécurité. La base de données comprend tous les outils de production de rapport sur les normes de l'industrie, de requête et d'analyse graphique. Le CDR a la capacité de stocker et de consolider tous les renseignements de différentes sources de données existantes requis pour les activités liées à la cyberdéfense. Tous les renseignements sont normalisés dans un modèle de données global et unifié selon les normes, puis rendus disponibles à toutes les applications qui en ont besoin. Le but principal du CDR est de consolider les renseignements à partir des outils et des produits existants qui ne sont pas interopérables et de permettre une corrélation globale pour les différentes activités liées à la cyberdéfense. Le composant est aussi la base pour produire une capacité de COD interopérable modulaire, flexible et agile. Ce CDR rassemble, stocke et maintient toutes les sources et les renseignements cybernétiques de sources ouvertes et de services gouvernementaux, alliés, militaires et contractuels tout en fournissant une vue d'ensemble complète, exacte et à jour des menaces autant de nature cybernétique que non liée au domaine cybernétique du MDN et des FAC. Les sources de renseignement engloberont des flux sans classification à TRÈS SECRET. Pour des raisons de sécurité, cette base de données sera maintenue séparée du CDR. La base de données comprend tous les outils de production de rapport sur les normes de l'industrie, de requête et d'analyse graphique.
7	Cyberentités et découverte d'événements	Ce composant découvre, recueille et stocke toutes les données sur toutes les cyberentités et tous les cyberévénements, puis les stocke dans le CDR. Pour l'entrée manuelle des données, le système utilise le COD. Le système découvre et recueille des données selon une routine prédéfinie, soit automatiquement selon les modifications apportées aux données sur les cyberentités pour répondre aux alertes des systèmes de surveillance actuels ou à la demande d'un cyberopérateur. Le sous-système utilise la collection et la rétention de données de trafic brutes, le suivi du trafic du réseau et la détection d'événements en temps réel, le suivi de l'hôte et la détection d'événements en temps quasi réel, et le suivi des activités et la détection d'événements en temps quasi réel. Le tout est appuyé par une capture de l'ensemble des paquets à des points clés désignés dans le cyberespace du MDN et des FAC, où et quand il est possible.

ANNEXE B – FACTEURS OPÉRATIONNELS

Série	Facteur	Besoin	Résultat
1	Sensibilisation La possibilité de rassembler, de fusionner et d'afficher des informations de qualité et en temps opportun dans différents domaines cybernétiques.	La connaissance du domaine cybernétique est essentielle à la prise de décisions en matière de cybersécurité et de défense. Des données provenant de sources multiples sont nécessaires pour visualiser le domaine cybernétique du MDN et des FAC, afin de faciliter le commandement et le contrôle de la cyberforce. Cela permet d'identifier les anomalies ou les tendances qui peuvent être négligées si elles sont limitées par un domaine unique.	Une visualisation dégagée, persistante et maniable du cyberespace du MDN et des FAC qui permet l'analyse et la prise de décision.
2	Réactivité La capacité d'anticiper et d'intervenir lorsque cela s'avère nécessaire.	Le MDN et les FAC doivent être en mesure d'exercer un contrôle faisant autorité sur le cyberespace (les réseaux internes des FAC inclus dans la portée du projet de CD-DAR, le cyberespace est défini dans le glossaire de l'AR) à tous les niveaux tactique, opérationnel et stratégique.	Afin de déterminer et d'atténuer les menaces, les attaques et les vulnérabilités, le MDN et les FAC disposent d'une capacité proactive qui analyse en permanence le cyberespace et prend en charge les interventions.
3	Flexibilité et évolutivité Il s'agit de la capacité de répondre à l'ennemi et de soutenir les plans d'action amis et de maintenir la liberté de manœuvre dans le cyberespace du MDN et des FAC.	Une capacité opérationnelle qui est déployable, capable de fonctionner dans le contexte opérationnel des FAC; évolutive, modulaire et facilement élargie; et qui peut fonctionner efficacement dans un environnement interdomaines.	Une capacité efficace, évolutive et durable dans l'ensemble des scénarios opérationnels des FAC et fonctionnelle dans l'environnement de cyberdéfense du MDN et des FAC.

Série	Facteur	Besoin	Résultat
4	Résilience La capacité de se remettre des changements de réseau, des attaques, des dommages ou des effets déstabilisants dans l'environnement cybernétique, opérationnel et naturel, et de s'y adapter.	Une capacité qui peut facilement se remettre d'une situation opérationnelle, ou s'y adapter, tout en conservant une capacité de cybersécurité et de capacité de défense de qualité.	Une capacité résiliente qui peut constamment soutenir les opérations de réseau, la cybersécurité et les COD dans un environnement hautement contesté.
5	Innovateur La possibilité de modifier la capacité en fonction du rythme actuel de l'évolution de la technologie	Une capacité efficace sur le plan opérationnel qui évolue continuellement et exploite les possibilités émergentes (telles que l'intelligence artificielle [IA], l'apprentissage par machine [AM] et les analyses avancées) grâce à de nouveaux processus, des outils évolutifs et une formation adaptative. Il faut mettre en œuvre une solution qui peut suivre le rythme de ce changement rapide, y compris, mais sans s'y limiter, l'utilisation de méthodes de passation de marchés relationnelles qui tirent parti de la capacité des fournisseurs de l'industrie à fournir des solutions en temps opportun par une conversation continue.	Tout au long de son cycle de vie, il s'agit d'une capacité de premier ordre qui peut être facilement mise en œuvre pour faire face à l'environnement changeant, à la mission et à la menace.
6	Interopérabilité Toutes les entités de force se connectent sans difficulté ou s'échangent de l'information.	Une capacité conjointe pour la fusion ou l'échange de sources de données multiples dans les domaines du MDN et des FAC, avec des alliés clés et avec l'infrastructure du cyberespace des partenaires. (GC, États-Unis, Groupe des cinq, Organisation du Traité de l'Atlantique Nord [OTAN], Sécurité publique, Services partagés Canada, le Centre de la sécurité des télécommunications [CST] et le secteur privé).	Une capacité technique et d'information qui permet des opérations harmonieuses au sein du MDN et des FAC et avec nos principaux alliés et partenaires, contribuant à la cybersécurité plus large du GC.

a. Découverte d'actifs cybernétiques – Il est actuellement difficile de découvrir et de suivre tous les actifs de réseau et de distinguer les éléments connus des éléments nouveaux (et inconnus). Les failles de logiciel et la configuration inadéquate des composants du système sont des vulnérabilités importantes des systèmes d'information qui permettent l'exploitation du système. Il y a des capacités mineures déployées de façon sporadique dans l'ensemble du MDN et des FAC, mais rien ne produit ou ne s'harmonise avec une solution d'entreprise pour la cyberforce du MDN et des FAC;

b. Cyberanalyse – Il est actuellement difficile de distinguer le trafic régulier provenant de dispositifs connus du trafic suspect ou du trafic provenant de dispositifs nouveaux et inconnus. Les capacités actuelles de cyberopérations de défense (COD) sont principalement manuelles et insuffisantes pour la complexité du domaine cybernétique du MDN et des FAC ou les tactiques utilisées par nos adversaires potentiels. Les capteurs sont insuffisants, et lorsqu'ils détectent des indications d'activités malveillantes possibles, les analystes doivent assembler manuellement les données et essayer de comprendre l'étendue de l'atteinte, identifier l'acteur malveillant et l'article ou l'emplacement ciblé, et déterminer les répercussions opérationnelles. Le MDN et les FAC ont quelques solutions, mais aucune n'a été spécialement conçue pour effectuer des analyses à l'échelle et du type de CD-DAR qui sera conçu pour fournir ce qui suit :

c. Cyberintervention – La capacité de réagir au trafic inconnu et d'éliminer les menaces est difficile. Les systèmes actuels du domaine cybernétique du MDN et des FAC ne peuvent pas fournir les données avec l'information opérationnelle et le renseignement actuels qui appuient les processus décisionnels du commandement; cela alourdit les processus actuels, rend leur intégration insuffisante et leur confère un manque de réactivité. La solution CD-DAR permettra au Cybercommandant et à la Cyberforce de choisir des technologies plus autonomes afin qu'ils aient le plein contrôle des actions réactives lorsqu'ils font face à des événements cybernétiques.

d. Cybercommandement et contrôle – Le commandement et le contrôle des cyberactions dans l'environnement du domaine cybernétique du MDN et des FAC représentent un défi. Les capacités actuelles ne permettent pas le commandement et le contrôle des cyberactions défensives dans l'ensemble de nos réseaux les plus importants. Les systèmes du domaine cybernétique du MDN et des FAC ne peuvent pas fournir les données avec l'information opérationnelle et le renseignement qui aident les processus décisionnels du commandement. La solution CD-DAR améliorera notre capacité d'exécuter le commandement et le contrôle d'éléments cybernétiques dans l'environnement du domaine cybernétique du MDN et des FAC, grâce à des interfaces normalisées et à des flux de travail automatisés à l'appui;

e. Intégration – L'information des COD du MDN et des FAC n'est pas actuellement intégrée au système d'entreprise. L'intégration de renseignements propres au cyberespace pour le cybercommandant et la cyberforce est actuellement possible, mais les capacités de CD-DAR permettront un processus plus homogène et une intégration plus rapide;

f. Interopérabilité – Il est difficile d'échanger des vecteurs de cybermenace et d'analyser l'information entre les ministères internes, les domaines externes ou avec d'autres pays. Les mesures clés en matière de cyberdéfense, comme l'échange de vecteurs de cybermenace, l'accès à des sources de données externes amies et l'accès à l'information d'analyse au moyen de

systèmes internes[13], doivent être menées de façon transparente. Toutes les entités de la force doivent être en mesure de se connecter et de fournir l'échange d'information requis entre elles. Les capacités, comme l'application Cyber Incident and Information Coordination System ou la Malware Information Sharing Platform, ne sont pas compatibles avec la capacité que la solution CD-DAR fournira au Cybercommandant et à la force;

g. Résilience – Il est difficile ou impossible de surveiller les environnements débranchés, intermittents et limités (DIL). Le modèle actuel est manuel, axé sur l'organisation et a une réactivité limitée. Nos réseaux n'ont pas de résilience cybernétique conçue, comme la capacité d'effectuer une surveillance et une analyse localisées et d'appuyer la prise de décisions responsables dans des réseaux régionaux déconnectés, intermittents et limités géographiquement même lorsqu'ils sont déconnectés d'un point de gestion central. La solution CD-DAR sera résiliente et capable de fonctionner dans des environnements déconnectés, intermittents et limités géographiquement;

h. Évolution continue – Tout changement dans les politiques, la technologie, la portée, les flux de travail, l'instruction collective, le développement d'outils cybernétiques ou les menaces, a une grande incidence sur les systèmes, les infrastructures et les politiques connectés, ce qui réduit ou désactive la fonctionnalité. Par conséquent, le fait de veiller à ce que les capacités conjointes de cybersécurité et de défense soient maintenues permet d'exploiter les fonctions opérationnelles interarmées. Cela doit se faire dans le cyberenvironnement, tout en veillant à ce que les améliorations ou les ajouts à ces cybercapacités soient mis en œuvre sans avoir d'incidence sur la base de référence de l'infrastructure de TI;

i. Souplesse – Il n'y a pas de capacité évolutive ou durable efficace dans tous les engagements opérationnels des FAC qui sont fonctionnels dans les environnements de cybersécurité et de défense du MDN et des FAC.

[13] De même que les systèmes et les environnements de réseau assignés de certains autres ministères et organismes gouvernementaux, pays du Groupe des cinq (Gp5), pays de l'Organisation du Traité de l'Atlantique Nord (OTAN) et autres organisations externes

Annexe B: Critères d'évaluation obligatoires

1. Critères techniques obligatoires

Le répondant doit satisfaire aux critères d'évaluation technique obligatoires précisés dans le tableau 1 de l'annexe B de l'ISQ. Tous les critères d'évaluation énumérés dans le tableau 1 sont obligatoires et sont tous assujettis au processus de conformité des soumissions par étapes. Le répondant doit fournir les documents nécessaires afin de démontrer le respect de ces exigences. Chaque critère technique obligatoire doit être traité séparément.

Projets : Dans les cas où le répondant doit inclure une description de projets :

(i) un projet doit avoir été achevé par le répondant lui-même et ne peut pas inclure l'expérience d'un sous-traitant proposé ou d'un affilié du répondant;

(ii) un projet doit avoir été achevé à la date de clôture de l'IQ;

(iii) plus d'un (1) projet de référence peut être utilisé pour répondre aux critères d'évaluation;

(iv) un projet doit être en exploitation, pas en recherche et développement (R&D) ou en environnement d'essai;

(v) un projet doit avoir été réalisé au cours des cinq (5) dernières années;

(vi) un projet peut être fait en tant que coentreprise, mais les répondants doivent identifier les composants dont ils étaient responsables;

(vii) un projet peut être utilisé pour satisfaire plusieurs critères;

(viii) les répondants doivent identifier clairement leur rôle, leurs responsabilités et les livrables de leur contrat de manière aussi détaillée que possible;

(ix) le répondant doit identifier quels ont été les résultats obtenus, les livrables atteints, dans le cadre de leur contrat et s'ils ont été atteints dans les limites de la portée, du budget et de l'échéancier.

Les répondants doivent fournir le formulaire 2 – Formulaire de vérification des projets cités en référence, pour chaque projet déclaré en réponse aux exigences obligatoires correspondantes.

Les répondants devraient seulement fournir les projets cités en référence demandés, comme indiqué dans chaque exigence obligatoire. Si le nombre de projets cités en référence est supérieur au nombre demandé, les répondants devront préciser les projets cités en référence qui s'appliquent aux exigences obligatoires correspondantes.

Le fournisseur doit fournir les renseignements suivants pour chaque projet cité en référence :

a. nom du projet
b. une brève description de l'objectif du projet
c. la valeur du projet
d. en coentreprise ou à titre de fournisseur unique
e. la valeur du contrat (avec le fournisseur)
f. la durée du projet (mois/année)
g. la durée du contrat (mois/année)

ébauche

h. le niveau d'effort du projet (année-personne – bureau de projet et expert en la matière)
i. le niveau d'effort du contrat (année-personne – bureau de projet et expert en la matière)
j. la portée de la capacité (nombre d'usagers et points terminaux)
k. l'énoncé des besoins du projet et sa portée
l. la classification du projet
m. les références et coordonnées

2. Formulaire 2 – Formulaire de vérification des projets cités en référence

Instructions à l'intention des fournisseurs :

(a) Les fournisseurs doivent soumettre un formulaire de vérification pour chaque projet cité en référence, en réponse aux exigences obligatoires du tableau 1 de l'annexe B de l'ISQ.

(b) Si les renseignements demandés dans le présent formulaire n'accompagnent pas la réponse du répondant à l'ISQ, ils doivent être fournis sur demande de l'autorité contractante dans le délai précisé.

(c) Le Canada peut communiquer avec la personne-ressource du client, indiquée pour le projet cité en référence, afin de valider les renseignements fournis.

ébauche

Formulaire 2 – Formulaire de vérification des projets cités en référence

#	Response		
(a)	Numéro du critère obligatoire (voir table 1 de l'annexe B)		
(b)	Nom légal complet du fournisseur (si le fournisseur est une coentreprise, le nom légal complet du membre de la coentreprise pour le projet référencé)		
(c)	Description du projet et du contrat (spécifique au répondant), la valeur en dollars canadiens, la durée (indiquer le mois et l'année) et la cote de sécurité du projet référencé		
(d)	Nom de l'organisation cliente pour le projet référencé		
(e)	Nom du contact client et ses coordonnées pour le projet référencé		
(f)	Organisation cliente et affiliation du contact client avec le fournisseur (ou membre de la coentreprise). Veuillez indiquer: Ne sont pas affiliés Sont affiliés		
	Veuillez indiquer:	Ne sont pas affiliés	Sont affiliés
(g)	Nom de l'organisation pour laquelle le contact client travaille actuellement (si le contact client ne travaille plus pour l'organisation cliente identifiée pour le projet référencé)		
(h)	Titre du contact client (lorsqu'il travaillait pour le projet référencé)		
(i)	Numéro de téléphone actuel du contact client		
(j)	Adresse courriel actuelle du contact client		
(k)	Rôle du contact client dans le projet référencé		
(l)	Indiquez le nombre maximal d'utilisateurs et de points terminaux du projet référencé sur lequel seul le répondant a travaillé.		
	Nombre d'utilisateurs:	Nombre de points terminaux:	
(m)	Identifiez les composants dont vous étiez responsable: (Si le projet référencé était une coentreprise, veuillez identifier uniquement les composants pour lesquels le répondant était responsable)		
(n)	Identifier le niveau d'effort (année-personne – bureau de projet et expert en la matière) pour les composants du projet référencé dont vous étiez responsable		
(o)	Confirmer que le projet référencé se trouve dans un environnement d'exploitation (Oui/Non)		
(p)	Si le projet référencé est utilisé pour satisfaire plusieurs critères, veuillez fournir une ventilation du pourcentage pour les critères donnés alloués dans le cadre de l'échéancier du projet		
(q)	Pour le contrat dont relève le projet référencé, indiquer clairement le rôle, les responsabilités et les produits livrables du répondant de la façon la plus détaillée possible		

ébauche

3. Table 1 - Critères d'évaluation technique obligatoires

Les termes ou mots en italique sont définis dans Table 2 - Définitions

Serial	Criteria	Évaluation	Preuve requise (au cours des cinq années qui ont précédé la date de clôture de l'ISQ)
1	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de gestion de l'information / technologie de l'information (GI/TI) au cours des cinq (5) dernières années, qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique*, et la prestation d'au moins 12 mois de *soutien de stabilisation* déployées : **a. Dans des *réseaux GI/TI complexes* d'au moins 10 000 *points terminaux*,** **b. Pour un ou plusieurs pays du Groupe des cinq (Gp5) [Australie, Canada, Nouvelle-Zélande, Royaume-Uni, États-Unis] ou pays membres de l'OTAN.**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) années dans le cadre duquel il a *mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 1.
2	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI au cours des cinq (5) dernières années, qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique*, et la prestation d'au moins 12 mois de *soutien de stabilisation* qui offrent des capacités pour : **a. cibler tous les biens de gestion de l'information et de technologie de l'information (autorisés et non autorisés) dans un environnement *réseaux GI/TI complexes* désigné d'au moins 10,000 *points terminaux* et d'en faire le suivi;** **b. évaluer la vulnérabilité des biens, la configuration, les risques et l'application des correctifs;** **c. recueillir, conserver et analyser des renseignements sur les cybermenaces;** **d. détecter et analyser les activités suspectes, et fournir un contexte**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il a *mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 2.

ébauche

Serial	Criteria	Évaluation	Preuve requise (au cours des cinq années qui ont précédé la date de clôture de l'ISQ)
	pour les évaluations des risques et de la vulnérabilité; **e. exécuter les interventions en réponse aux menaces et les mesures correctives en *temps quasi réel*;** **f. fournir une *décision, analyse et réponse cybernétique* des systèmes de *réseaux de commandement et de contrôle* au moyen d'une *image commune de la situation opérationnelle* intégrée;** g. **offrir au moins 12 mois de *soutien de stabilisation*.**		
3	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI au cours des cinq (5) dernières années, qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* **qui démontrent TOUS les éléments suivants dans un environnement de *réseaux GI/TI complexes* d'au moins 10,000 *points terminaux*, et de la prestation d'au moins 12 mois de *soutien de stabilisation*, au cours des cinq (5) dernières années:** **a. collecte, rétention, détection et analyse des données en continu, et de fournit un contexte pour les évaluations des risques et des vulnérabilités en *temps quasi réel*;** **b. capacité à normaliser les flux de données liés aux cybermenaces et les données d'analyses, et à les intégrer dans un format commun afin de les analyser et d'établir une *image commune de la situation opérationnelle*;** **c. *analyse de données avancées* en utilisant:** **i. une amélioration des alertes de *cybersécurité* à partir :** **1) des renseignements sur les menaces,** **2) des renseignements sur les entités externes,** **3) des renseignements sur les biens internes,** **4) des renseignements sur la détection des événements et**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il a *mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 3.

ébauche

Serial	Criteria	Évaluation	Preuve requise (au cours des cinq années qui ont précédé la date de clôture de l'ISQ)
	l'intervention, **5) des renseignements de l'analyse du trafic sur le réseau,** **6) de l'historique des activités;** **7) de l'analyse du comportement des utilisateurs et des entités;** **ii. une amélioration des données sur les incidents de *cybersécurité*, à partir:** **1) des renseignements sur les menaces,** **2) des incidents antérieurs,** **3) des incidents similaires,** 4) **de la détection de signature et la détection heuristique.**		
4	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI au cours des cinq (5) dernières années, qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique*, et la prestation d'au moins 12 mois de *soutien de stabilisation* – **en utilisant la détermination *adaptative* et *dynamique*, le contrôle et l'éradication des menaces au moyen de capacités avancées de cyberdéfense en *temps quasi réel* dans un environnement *réseaux GI/TI complexes* désigné d'au moins 10,000 *points terminaux* au cours des cinq (5) dernières années.**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il a *mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 4.
5	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI au cours des cinq (5) dernières années, qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique*, et la prestation d'au moins 12 mois de *soutien de stabilisation* – **en établissant un dépôt de données qui prend en charge le stockage, la récupération et le traitement des données structurées et non structurées pour un *réseaux GI/TI complexes* d'au moins 10,000**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il a *mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 5.

ébauche

Serial	Criteria	Évaluation	Preuve requise (au cours des cinq années qui ont précédé la date de clôture de l'ISQ)
	***points terminaux* et effectuer des *analyses de niveau 2* afin de permettre l'aide à la prise de décisions grâce à l'exécution automatisée et assistée des réponses.**		
6	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI au cours des cinq (5) dernières années, qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique*, et la prestation d'au moins 12 mois de *soutien de stabilisation* **pour des *réseaux GI/TI complexes* d'au moins 10,000 *points terminaux* au sein de composants de réseau mondialement répartis sur au moins deux (2) continents, où :** a. **la connectivité n'est pas disponible, n'est pas fiable ou à faible capacité (bande passante) [par exemple, communications par satellite (Mbps), navires (Kbps)];** b. **la resynchronisation des données avec l'environnement durable est automatique dès que la connectivité est rétablie.**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il *a mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 6.
7	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique*, et la prestation d'au moins 12 mois de *soutien de stabilisation* **pour des *réseaux GI/TI complexes* d'au moins 10,000 *points terminaux* offrant les fonctionnalités d'interopérabilité suivantes au sein des autres ministères du gouvernement du Canada et des nations du Groupe des cinq (alliés) au cours des cinq (5) dernières années, mais sans s'y limiter:** **a. la capacité de partager de façon transparente des renseignements tels que des vecteurs de menaces, des résultats d'analyses, etc., avec des partenaires clés tels les autres ministères et les alliés;** **b. de collecte centralisée des renseignements sur les menaces;**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il a *mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 7.

ébauche

Serial	Criteria	Évaluation	Preuve requise (au cours des cinq années qui ont précédé la date de clôture de l'ISQ)
	c. fusion et déduplication des renseignements sur les menaces; **d. recherche et analyse graphique des indicateurs;** **e. stockage de renseignements sur les menaces lisibles par machine et non structurés;** f. **transfert de renseignements sur les menaces vers des outils externes;** g. **interfaces et mécanismes d'échange de renseignements sur les menaces avec d'autres organisations (dans des formats comme SCAP, STIX et JSON).**		
8	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI pour lequel le répondant a mis en œuvre les technologies émergentes suivantes dans le cadre des principales solutions de *cybersécurité* et *décision, analyse et réponse cybernétique* **pour au moins 10,000 *points terminaux* au cours des cinq (5) dernières années:** ***a. intelligence artificielle;*** ***b. apprentissage automatique;*** ***c. infonuagique;*** ***d. analyse des modèles de comportement;*** ***e. mégadonnées.*** **Le *répondant* est prié d'identifier toutes autres technologies émergentes que le gouvernement du Canada devrait prendre en considération dans sa mise en œuvre.**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années pour lequel le répondant a intégré des solutions de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 8.
9	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI qui comprenait la conception, l'élaboration et la prestation de **solutions intégrées de formation et de mise en pratique destinées à des opérateurs et à des spécialistes de la maintenance de systèmes de *cybersécurité* et *décision, analyse et réponse cybernétique* (matériel et logiciel) pour au moins 10,000 *points terminaux* au cours des cinq (5)**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il a élaboré et fourni des solutions de formation et de mise en pratique pour le critère 9.

ébauche

Serial	Criteria	Évaluation	Preuve requise (au cours des cinq années qui ont précédé la date de clôture de l'ISQ)
	dernières années.		
10	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique*, et la prestation d'au moins 12 mois de *soutien de stabilisation* **pour des *réseaux GI/TI complexes* d'au moins 10,000 *points terminaux* au cours des cinq (5) dernières années:** a. **des environnements de sécurité à niveaux multiples (désignés, secrets, très secrets);** b. **des environnements de sécurité à restrictions multiples (au sein du même niveau de sécurité).**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il a *mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 10.
11	Le *répondant* doit avoir *mis en œuvre avec succès* au moins un (1) *projet complexe* de GI/TI qui comprenait la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation de solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique*, et la prestation d'au moins 12 mois de *soutien de stabilisation* – **pour l'administration et la gestion de la collecte de données à partir de sources *hétérogènes* et la gestion de la configuration de grandes collections de données dans des *réseaux GI/TI complexes* d'au moins 10 000 *points terminaux* au cours des cinq (5) dernières années.**	Réussite / échec	Le *répondant* doit soumettre au moins un (1) projet de référence réalisé au cours des cinq (5) dernières années dans le cadre duquel il a *mis en œuvre avec succès* des solutions commerciales ou gouvernementales de *cybersécurité* et *décision, analyse et réponse cybernétique* pour le critère 11.

ébauche

Table 2 Définitions

Terme	Définition
Adaptatif	Capacité à évoluer, à s'adapter ou à se modifier en conséquence.
Analyse de données avancée	L'examen autonome ou semi-autonome de données ou de contenu à l'aide de techniques et outils sophistiqués, généralement au-delà de ceux de la veille stratégique traditionnelle, pour découvrir des connaissances plus approfondies, faire des prévisions ou formuler des recommandations.
Analyse de niveau 2	L'analyse de niveau 2 fournit une analyse plus approfondie et met l'accent sur le soutien aux incidents et le traitement des alertes à partir du niveau 1. Les analystes de niveau 2 coordonnent les résultats de la surveillance de la sécurité avec l'équipe du renseignement de menace, les fournisseurs partenaires et avec des points de contact spécifiques pour obtenir une analyse plus large des données sur les évènements et leur impact sur les environnements désignés.
Analyse des modèles comportementaux	L'analyse comportementale utilise l'apprentissage automatique, l'intelligence artificielle, les mégadonnées et les analyses pour identifier les comportements malveillants et furtifs en analysant les différences subtiles dans les activités quotidiennes normales afin de stopper de manière proactive les cyberattaques avant que les attaquants n'aient la capacité d'exécuter pleinement leurs plans destructeurs. L'analyse des modèles de comportement commence par la surveillance du comportement, qui dans un contexte de cybersécurité consiste à : Enregistrement des évènements et des activités d'un système et de ses utilisateurs. Les évènements enregistrés sont comparés aux politiques de sécurité et aux bases de référence comportementales pour évaluer la conformité et/ou découvrir les violations. La surveillance comportementale peut comprendre le suivi des tendances, l'établissement de seuils et la définition de réponses. Le suivi des tendances peut révéler quand les erreurs augmentent nécessitant des services de soutien technique, quand des niveaux de charge anormaux se produisent indiquant la présence de code malveillant, ou quand les niveaux de travail de production augmentent indiquant un besoin d'augmenter la capacité. Les seuils servent à définir les niveaux d'activité ou les évènements au-dessus desquels il y a lieu de s'inquiéter et qui nécessitent une intervention. Les niveaux inférieurs au seuil sont enregistrés mais ne déclenchent pas de réponse. Les réponses peuvent consister à résoudre des conflits, à traiter des violations, à prévenir les temps d'arrêt ou à améliorer les capacités.
Apprentissage automatique	Processus par lequel une unité fonctionnelle améliore son rendement en acquérant de nouvelles connaissances ou compétences, ou en réorganisant les connaissances ou les compétences existantes.
Auto-guérison	Dans le monde informatique, les systèmes d'auto-guérison sont décrits comme « tout dispositif ou système qui a la capacité de percevoir qu'il ne

ébauche

Terme	Définition
	fonctionne pas correctement et, sans aide externe, de faire les ajustements nécessaires pour se rétablir en fonctionnement normal ». Un système, qui devrait toujours être opérationnel comme prévu.
Biens électroniques	Ensemble de biens (logiciel, matériel et utilisateurs [autorisés et non autorisés]) connectés au réseau de commandement (sans compter la gestion de l'identité, des justificatifs d'identité et de l'accès pour les utilisateurs).
Connaissance de la situation	Connaissance des éléments de l'environnement opérationnel nécessaire à la prise de décisions éclairées.
Cybersécurité	Ensemble de technologies, de processus, de pratiques et de mesures d'intervention et d'atténuation conçues pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou l'accès non autorisé afin d'assurer la confidentialité, l'intégrité et la disponibilité.
Décision, analyse et réponse cybernétique	Atteinte d'une caractérisation précise d'un bien électronique ou d'une faiblesse ou menace relative à l'utilisation, et prise de mesures de cyberdéfense et de cybersécurité approuvées afin de préserver la liberté d'action.
Déployé	Capacité à l'appui d'une base expéditionnaire (dispersée géographiquement et fonctionnant la plupart du temps dans un environnement de menace) employant et soutenant les forces opérationnelles lors de missions.
Dynamique	Caractéristique d'un attribut de données, dont les valeurs ne peuvent être établies que durant l'exécution d'une partie ou de l'ensemble d'un programme.
État des biens	État déterminé par l'évaluation des attributs des biens sur les plans de la vulnérabilité, de la configuration, du risque et de l'application des correctifs.
Hétérogène	• Équipement réseau provenant de divers fournisseurs ou de différentes générations technologiques (ancien/moderne) • Applications logicielles : de différents fournisseurs, de version ou de niveaux de correctifs divers • Diverses sources de données structurées/non structurées
Image commune de la situation opérationnelle	Représentation dynamique d'information partagée pouvant être adaptée pour faciliter la connaissance de la situation, la planification collaborative, la prise de décisions et la réponse.
Infonuagique	L'infonuagique est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un bassin partagé de ressources informatiques configurables (p. ex., réseaux, serveurs, stockage, applications et services), qui peuvent être rapidement provisionnées et diffusées avec un effort de

ébauche

Terme	Définition
	gestion minimal ou interaction des prestataires de services.
Intelligence artificielle	Capacité d'un ordinateur à effectuer des fonctions associées à la logique humaine telles que le raisonnement, l'apprentissage et l'auto-amélioration.
Liberté d'action	Une fois la tâche ou la mission établie et les ordres nécessaires transmis, les commandants subordonnés doivent pouvoir jouir d'un maximum de liberté d'action pour prendre l'initiative, exercer leur savoir-faire et mettre en application leur connaissance de la situation locale dans le cadre de la planification et de la conduite d'une opération, et ce, en ayant peu ou pas de contraintes.
Mégadonnées	Grand ensemble de données qui, en raison de la vitesse à laquelle il croît, est difficile à gérer à l'aide des outils logiciels traditionnels disponibles.
Mis en œuvre avec succès	État atteint lorsque le répondant a assuré la conception, l'élaboration, l'intégration, la mise en œuvre et la prestation d'un soutien de stabilisation dans le cadre d'un projet réalisé avec succès dans le respect des exigences et pour lequel les clients ont fourni une preuve d'acceptation; autrement, une lettre d'appui d'un client (fédéral) est acceptable.
Point terminal	Un point terminal est un dispositif informatique distant qui communique d'avant en arrière avec un réseau auquel il est connecté. Les ordinateurs portables, les ordinateurs de bureau, les téléphones mobiles, les tablettes, les serveurs et les environnements virtuels peuvent tous être considérés comme des points terminaux.
Projet complexe	Les projets complexes sont des projets caractérisés comme ayant de nombreux éléments sociaux et techniques différents à plusieurs niveaux qui sont interconnectés et interdépendants. Contrairement aux projets plus simples qui sont des efforts normalisés et bien définis dans des environnements prévisibles et stables, les projets complexes comportent généralement un degré élevé d'incertitude dans la définition des objectifs finaux, ils se déroulent souvent dans un environnement changeant et peuvent nécessiter l'apport de nombreux intervenants divers.
Relation contractuelle	Une lettre d'appui d'un membre de la coentreprise constitue une preuve acceptable d'une relation contractuelle.
Répondant	Terme faisant référence à l'intégrateur de système principal, à la coentreprise ou au membre de la coentreprise proposé dans le cadre du processus d'approvisionnement du projet Cyberdéfense – Décision, Analyse et Réponse (CD-DAR).
Réseau de commandement et de contrôle	Réseau sur lequel un commandant exerce son autorité sur les forces affectées, allouées ou détachées pour la conduite d'une mission.

ébauche

Terme	Définition
Réseau GI/TI complexe	Les réseaux de GI/TI dit « complexes » ont des propriétés distinctes qui découlent de l'interaction des systèmes complexes qu'ils comprennent, comme de l'équipement réseau important, distribué à l'échelle mondiale, dynamique, adaptable, hétérogène (ancien / moderne, divers fournisseurs), des applications hétérogènes (version du logiciel, licences, fournisseurs), source de données hétérogènes (structurées / non-structurées), auto-guérison (un système, qui devrait toujours être opérationnel comme prévu), connectivité intermittente, faible bande passante (par exemple, communications par satellite (Mbps), Navires (Kbps), etc.) et la latence.
Soutien de stabilisation	Soutien continu pendant au moins 12 mois, à partir du moment où le ou les groupes de clients ont commencé à utiliser la capacité cybernétique jusqu'au moment où la capacité cybernétique a été entièrement mise en œuvre, au minimum.
Soutien de troisième ligne	Capacités de soutien fournies à une force militaire au sein d'un théâtre d'opérations ou à des installations établies le long des lignes de communication stratégiques.
Système complexe	Les systèmes complexes sont des systèmes dont le comportement est intrinsèquement difficile à modéliser en raison des dépendances, des compétitions, des relations ou d'autres types d'interactions entre leurs parties ou entre un système donné et son environnement. Les systèmes qui sont «complexes» ont des propriétés distinctes qui découlent de ces relations, telles que la non-linéarité, l'émergence, l'ordre spontané, l'adaptation et les boucles de rétroaction, entre autres.
Temps quasi réel	Qualificatif appliqué à l'acheminement des données ou des informations qui s'effectue sans délai si ce n'est celui du traitement automatique et de la transmission électronique. Cela implique que les délais sont limités aux capacités du support de transport de données.
Voies de communication	Ensemble des itinéraires terrestres, maritimes, fluviaux ou aériens qui relient une force opérationnelle à une ou à plusieurs bases d'opérations, et par lesquels le matériel et les renforts sont acheminés.

ébauche

Annexe C : Exigences relatives à la sécurité

Les trois sections suivantes décrivent en détail les exigences de sécurité pour chaque étape du processus d'achat, y compris le contrat. Il s'agit des exigences de sécurité prévues en fonction des listes de vérification des exigences relatives à la sécurité (LVERS) incluses dans la présente annexe. Le Canada se réserve le droit de modifier les exigences de sécurité, au besoin.

1.1 Exigences de sécurité pour l'ISQ

a) L'ISQ ne comporte aucune exigence relative à la sécurité.

b) Il n'est pas nécessaire qu'un fournisseur détienne une cote de sécurité pour devenir un fournisseur qualifié.

c) Il y a des exigences de sécurité pour la phase de diligence raisonnable, la DP et le contrat.

d) À titre d'information, les fournisseurs doivent prendre note que le processus d'obtention des niveaux d'autorisation de sécurité exigés peut être long et qu'il dépend du niveau de sécurité requis. La responsabilité d'obtenir ces attestations de sécurité incombe entièrement aux fournisseurs.

Les fournisseurs qui ne détiennent pas actuellement les attestations de sécurité du personnel et les attestations de sécurité de l'organisation auprès du gouvernement fédéral canadien, ou encore, les fournisseurs qui ne respectent pas les exigences relatives à la sécurité prévues qui sont décrites dans les sections 1.2 et 1.3 devraient entreprendre tôt le processus d'obtention de l'attestation de sécurité en communiquant avec les responsables du Programme de la sécurité industrielle indiqué sur le site Web de TPSGC (https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html).

ébauche

1.2 Exigences de sécurité pour la phase 3 – Diligence raisonnable et la phase 4 – DP

Les exigences de sécurité suivantes (listes de vérification des exigences relatives à la sécurité [LVERS] et les clauses connexes prévues par le Programme de sécurité des contrats) s'appliquent à la phase de diligence raisonnable et à la phase de la DP et sont requises pour y participer pleinement. Les fournisseurs préqualifiés qui ne satisfont pas à ces exigences en matière de sécurité à la date de publication de la DP définitive seront retirés de la liste des fournisseurs qualifiés.

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:

DOSSIER TPSGC Nº W6369-20-CY06 / DP

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une cote de sécurité d'installation valable au niveau NATO SECRET, ainsi qu'une: cote de protection des documents approuvée au niveau SECRET et NATO SECRET, délivrées par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC).

2. Ce contrat comprend un accès à des marchandises contrôlées. Avant d'avoir accès, le soumissionnaire doit être inscrit au Programme des Marchandises Contrôlées de Travaux publics et Services gouvernementaux Canada (TPSGC).

3. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITÉ en vigueur, délivrée ou approuvée par le PSC, TPSGC

4. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS ou PROTEGÉS portant la mention "CITOYENS CANADIENS SEULEMENT", dont l'accès est réglementé, doivent être citoyens du Canada et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.

5. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS CANADIENS RESTREINTS ou PROTÉGÉS CANADIENS RESTREINTS, ou à des établissements dont l'accès est réglementé, doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.

6. Les membres du personnel de l'entreprise qui doivent avoir accès aux biens ou aux renseignements OTAN NON-CLASSIFIÉS doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande, mais n'ont pas besoin d'avoir une attestation de sécurité ; toutefois, l'entrepreneur doit s'assurer que de tiers n'auront pas accès aux renseignements OTAN NON-CLASSIFIÉS et que le principe du « besoin de savoir », sera appliqué.

7. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens NATO DIFFUSION RESTREINTE doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande et doivent TOUS détenir une cote de FIABILITÉ ou son

ébauche

équivalent en vigueur, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

8. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS OTAN, ou à des établissements dont l'accès est réglementé doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau NATO SECRET, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

9. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS ÉTRANGERS ou PROTÉGÉS ÉTRANGERS, ou à des établissements dont l'accès est réglementé, doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.

10. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens COMSEC, doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande et détenir une cote de sécurité du personnel valable proportionné avec les renseignements ou les biens qui seront accédés, avoir un besoin de connaitre et ont été soumis à une séance d'information COMSEC et ont signé un certificat de séance d'information COMSEC. L'accès par des étrangers, nationaux ou des résidents étrangers doit être approuvé par les Services à la Clientèle Chef de TI à CSTC sur une base de cas-par-cas.

11. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données au niveau CLASSIFIÉS/PROTÉGÉS tant que le PSC, TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau NATO SECRET et compris un lien électronique au niveau NATO SECRET.

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

13. Avant l'attribution du contrat, l'entrepreneur doit remplir un questionnaire sur la Participation, le contrôle et l'influence étrangers (PCIE) ainsi que les documents connexes indiqués dans les lignes directrices sur la PCIE destinées aux organisations. L'entrepreneur doit soumettre ces documents dûment remplis afin d'indiquer si une tierce partie (personne, entreprise ou gouvernement) peut accéder, sans en avoir l'autorisation, à des biens ou à des renseignements COMSEC, CLASSIFÉS DE L'OTAN ou CLASSIFÉS ÉTRANGERS. Travaux publics et Services gouvernementaux Canada (TPSGC) déterminera si le statut « Sans PCIE » ou « Avec PCIE » doit être attribué à l'entreprise de l'entrepreneur. Si le statut « Avec PCIE » est attribué à l'entreprise, TPSGC déterminera si des mesures d'atténuation existent ou doivent être prises par l'entreprise afin qu'elle puisse obtenir le statut « Sans PCIE par atténuation ».

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

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

ébauche

16. L’entrepreneur ou l’offrant doit respecter les dispositions :

    a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s’il y a lieu), reproduite ci-joint à l’Annexe C;

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

ébauche

1.3 Exigences de sécurité pour la phase 5 – Contrat

Les exigences de sécurité suivantes (listes de vérification des exigences relatives à la sécurité [LVERS] et les clauses connexes prévues par le Programme de sécurité des contrats) s'appliquent au contrat.

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:

DOSSIER TPSGC No W6369-20-CY06 / CONTRACT

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une cote de sécurité d'installation valable au niveau TRÈS SECRET et NATO SECRET, ainsi qu'une cote de protection des documents au niveau TOP SECRET et NATO SECRET délivrés par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC) et un compte COMSEC au niveau TOP SECRET, délivrée par la Centre de la sécurité des télécommunications Canada (CSTC).

2. Ce contrat comprend un accès à des marchandises contrôlées. Avant d'avoir accès, le soumissionnaire doit être inscrit au Programme des Marchandises Contrôlées de Travaux publics et Services gouvernementaux Canada (TPSGC).

3. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTEGÉS CANADIENS NON RESTREINTS, ou à des établissements dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITÉ, délivrée ou approuvée par le PSC, TPSGC.

4. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTEGÉS portant la mention "CITOYENS CANADIENS SEULEMENT", dont l'accès est réglementé, doivent être citoyens du Canada et doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITÉ, délivrée ou approuvée par le PSC, TPSGC.

5. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS CANADIENS RESTREINTS ou PROTÉGÉS CANADIENS RESTREINTS, ou à des établissements dont l'accès est réglementé, doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau TRÈS SECRET, SECRET, ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.

6. Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens TRÈS SECRET SIGINT, ou à des établissements dont l'accès est réglementé, doivent être citoyens du Canada et doivent TOUS détenir une cote de sécurité du personnel valable au niveau TRÈS SECRET SIGINT, délivrée par le Programme de sécurité des contrats (PSC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

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

8. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens NATO DIFFUSION RESTREINTE, doivent être citoyens du Canada, Étas-Unis ou Royaume-Unis, et doivent TOUS détenir une cote de FIABILITÉ ou son équivalent en vigueur,

ébauche

délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

9. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS OTAN, ou à des établissements dont l'accès est réglementé, doivent être citoyens du Canada, États-Unis ou Royaume-Unis, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau NATO SECRET, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

10. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS ÉTRANGERS ou PROTÉGÉS ÉTRANGERS, ou à des établissements dont l'accès est réglementé, doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.

11. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens COMSEC, doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande et détenir une cote de sécurité du personnel valable proportionné avec les renseignements ou les biens qui seront accédés, avoir un besoin de connaitre et ont été soumis à une séance d'information COMSEC et ont signé un certificat de séance d'information COMSEC. L'accès par des étrangers, nationaux ou des résidents étrangers doit être approuvé par les Services à la Clientèle Chef de TI à CSTC sur une base de cas-par-cas.

12. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données au niveau CLASSIFIÉS/PROTÉGÉS tant que le PSC, TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau NATO SECRET et compris un lien électronique au niveau NATO SECRET.

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

14. Avant l'attribution du contrat, l'entrepreneur doit remplir un questionnaire sur la Participation, le contrôle et l'influence étrangers (PCIE) ainsi que les documents connexes indiqués dans les lignes directrices sur la PCIE destinées aux organisations. L'entrepreneur doit soumettre ces documents dûment remplis afin d'indiquer si une tierce partie (personne, entreprise ou gouvernement) peut accéder, sans en avoir l'autorisation, à des biens ou à des renseignements COMSEC, CLASSIFÉS DE L'OTAN ou CLASSIFÉS ÉTRANGERS. Travaux publics et Services gouvernementaux Canada (TPSGC) déterminera si le statut « Sans PCIE » ou « Avec PCIE » doit être attribué à l'entreprise de l'entrepreneur. Si le statut « Avec PCIE » est attribué à l'entreprise, TPSGC déterminera si des mesures d'atténuation existent ou doivent être prises par l'entreprise afin qu'elle puisse obtenir le statut « Sans PCIE par atténuation ».

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

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

épuré

17. L’entrepreneur ou l’offrant doit respecter les dispositions :

    a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s’il y a lieu), reproduite ci-joint à l’Annexe C;

    b) du Manuel de la sécurité industrielle (dernière édition) et du Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein des entreprises du secteur privé canadien (ITSD-06A).

ébauche

1.4 Listes de vérification des exigences relatives à la sécurité [LVERS]

ébauche

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-RFP
Security Classification / Classification de sécurité
UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organizati Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM(IM)/DGIMPD/DPDCC
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

In this RFP phase, qualified suppliers will be required to access and store one or more classified Annexes that will be provided; information is classified up to SECRET and releasable only to Canadian citizens.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non	Yes / Oui ✓
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	No / Non ✓	Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non	Yes / Oui ✓
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	No / Non ✓	Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	No / Non ✓	Yes / Oui

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

Canada ✓	NATO / OTAN ✓	Foreign / Étranger ✓
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ✓	All NATO countries / Tous les pays de l'OTAN	No release restrictions / Aucune restriction relative à la diffusion
Not releasable / À ne pas diffuser ✓		
Restricted to: / Limité à : ✓	Restricted to: / Limité à : ✓	Restricted to: / Limité à : ✓
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :
FVEYs members only as applicable	FVEYs members only as applicable	FVEYs members only as applicable

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

PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ✓	PROTECTED A / PROTÉGÉ A ✓
PROTECTED B / PROTÉGÉ B ✓	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ✓	PROTECTED B / PROTÉGÉ B ✓
PROTECTED C / PROTÉGÉ C	NATO CONFIDENTIAL / NATO CONFIDENTIEL	PROTECTED C / PROTÉGÉ C
CONFIDENTIAL / CONFIDENTIEL	NATO SECRET / NATO SECRET ✓	CONFIDENTIAL / CONFIDENTIEL
SECRET / SECRET ✓	COSMIC TOP SECRET / COSMIC TRÈS SECRET	SECRET / SECRET ✓
TOP SECRET / TRÈS SECRET		TOP SECRET / TRÈS SECRET
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-RFP

Security Classification / Classification de sécurité
UNCLASSIFIED

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

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

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

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

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

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

Special comments:
Commentaires spéciaux :

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

10. b) May unscreened personnel be used for portions of the work? — No / Non ☑ Yes / Oui ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — No / Non ☐ Yes / Oui ☐
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-RFP

Security Classification / Classification de sécurité
UNCLASSIFIED

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRES SECRET
Information / Assets / Renseignements / Biens	✓	✓		✓	✓		✓	✓	✓							
Production																
IT Media / Support TI					✓		✓		✓							
IT Link / Lien électronique																

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-CONTRACT
Security Classification / Classification de sécurité
UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organizati... Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM(IM)/DGIMPD/DPDCC
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

In this Contract Award phase, the winning Bidder may require access to information that is collectively classified up to TOP SECRET - SIGINT as well as access to COMSEC assets, releasable to Canadian citizens only. The winning Bidder will also be required to store, process and exchange information with DND/CAF up to SECRET. Selected supplier personnel may also require access to designated restricted/classified areas and equipment to perform work as part of the contract fulfillment.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non	✓ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	✓ No / Non	Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non	✓ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	✓ No / Non	Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	✓ No / Non	Yes / Oui

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

Canada ✓	NATO / OTAN ✓	Foreign / Étranger ✓
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ✓	All NATO countries / Tous les pays de l'OTAN	No release restrictions / Aucune restriction relative à la diffusion
Not releasable / À ne pas diffuser ✓		
Restricted to: / Limité à : ✓	Restricted to: / Limité à : ✓	Restricted to: / Limité à : ✓
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :
FVEYS members only as applicable	CAN/UK/US members only as applicable	FVEYS members only as applicable

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

PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ✓	PROTECTED A / PROTÉGÉ A ✓
PROTECTED B / PROTÉGÉ B ✓	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ✓	PROTECTED B / PROTÉGÉ B ✓
PROTECTED C / PROTÉGÉ C	NATO CONFIDENTIAL / NATO CONFIDENTIEL	PROTECTED C / PROTÉGÉ C
CONFIDENTIAL / CONFIDENTIEL	NATO SECRET / NATO SECRET ✓	CONFIDENTIAL / CONFIDENTIEL
SECRET / SECRET ✓	COSMIC TOP SECRET / COSMIC TRÈS SECRET	SECRET / SECRET ✓
TOP SECRET / TRÈS SECRET ✓		TOP SECRET / TRÈS SECRET
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ✓		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-CONTRACT
Security Classification / Classification de sécurité
UNCLASSIFIED

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

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

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

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

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

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

Special comments:
Commentaires spéciaux :

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

10. b) May unscreened personnel be used for portions of the work? — No / Non: ✓ Yes / Oui: ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — No / Non: ☐ Yes / Oui: ☐
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRES SECRET
Information / Assets / Renseignements / Biens	✓	✓			✓	✓	✓		✓		✓	✓			✓	✓
Production																
IT Media / Support TI	✓	✓			✓		✓		✓							
IT Link / Lien électronique	✓	✓			✓		✓		✓						✓	

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

✓ No / Non ☐ Yes / Oui

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

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

✓ No / Non ☐ Yes / Oui

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

Annexe D: Formulaire de présentation de la réponse

<table>
<tr><th colspan="4">Invitation à se qualifier No. W6369-20CY06/A
Formulaire de présentation de la réponse</th></tr>
<tr><td>Dénomination sociale complète du répondant
Dans le cas d'une coentreprise, veuillez identifier tous les participants.</td><td colspan="3"></td></tr>
<tr><td rowspan="5">Représentant autorisé du répondant aux fins d'évaluation (p. ex., pour des précisions)</td><td>Nom</td><td colspan="2"></td></tr>
<tr><td>Titre</td><td colspan="2"></td></tr>
<tr><td>Adress</td><td colspan="2"></td></tr>
<tr><td>Téléphone</td><td colspan="2"></td></tr>
<tr><td>Courriel</td><td colspan="2"></td></tr>
<tr><td colspan="4">Numéro d'entreprise – approvisionnement (NEA) du répondant _____

Veuillez consulter les instructions uniformisées de SPC. Il est à noter que le NEA donné doit correspondre à la dénomination sociale utilisée dans la réponse. Si ce n'est pas le cas, le répondant sera déterminé en fonction de la dénomination sociale fournie, et le répondant devra fournir le NEA qui correspond à cette dernière.</td></tr>
<tr><td rowspan="4">Si le répondant fournit une réponse à l'ISQ à titre de coentreprise, il doit en indiquer la dénomination sociale complète, l'adresse et le numéro d'entreprise – approvisionnement (le cas échant) de la coentreprise. [Le répondant ajoutera des lignes si la coentreprise compte plus de deux membres].</td><td colspan="3">Dénomination sociale complète du membre de la coentreprise :</td></tr>
<tr><td colspan="3">Adresse du membre de la coentreprise :</td></tr>
<tr><td colspan="3">Dénomination sociale complète du membre de la coentreprise :</td></tr>
<tr><td colspan="3">Adresse du membre de la coentreprise :</td></tr>
<tr><td rowspan="4">Anciens fonctionnaires

Pour en savoir davantage, veuillez consulter l'article des instructions uniformisées de SPC intitulé « Ancien fonctionnaire ».

Si la réponse provient d'une coentreprise, veuillez fournir cette information pour chacun des participants.</td><td rowspan="2">Le répondant est-il un ancien fonctionnaire recevant une pension selon la définition des instructions uniformisées de SPC? Si oui, veuillez fournir les renseignements requis à la section des instructions uniformisées de SPC intitulée « Ancien fonctionnaire ».</td><td>Oui</td><td></td></tr>
<tr><td>Non</td><td></td></tr>
<tr><td rowspan="2">Le répondant est-il un ancien fonctionnaire ayant reçu une somme forfaitaire en vertu de la Directive sur le réaménagement des effectifs? Si oui, veuillez fournir les renseignements requis à la section des instructions uniformisées de SPC intitulée « Ancien fonctionnaire ».</td><td>Oui</td><td></td></tr>
<tr><td>Non</td><td></td></tr>
<tr><td rowspan="8">Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation

Pour en savoir davantage, veuillez consulter la section des Instructions uniformisées de SPC intitulée « Programme de contrats fédéraux pour l'équité en matière d'emploi ».

Veuillez cocher l'une des cases ou fournir l'information demandée. S'il s'agit d'une réponse d'un consortium, veuillez fournir cette information pour chacun des membres.</td><td colspan="2">Le répondant atteste qu'il n'a aucun effectif au Canada.</td><td></td></tr>
<tr><td colspan="2">Le répondant atteste qu'il est un employeur du secteur public.</td><td></td></tr>
<tr><td colspan="2">Le répondant atteste qu'il est un employeur sous réglementation fédérale, assujetti à la Loi sur l'équité en matière d'emploi.</td><td></td></tr>
<tr><td colspan="2">Le répondant atteste qu'il a un effectif combiné de moins de 100 employés (à temps plein, temps partiel ou temporaires) au Canada.</td><td></td></tr>
<tr><td colspan="2">Le répondant a un effectif combiné de 100 employés (à temps plein, temps partiel ou temporaires) ou plus au Canada.</td><td></td></tr>
<tr><td colspan="2">Le numéro de certificat est valide et à jour.</td><td></td></tr>
<tr><td colspan="2">Le répondant atteste qu'il a présenté l'accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168) aux responsables du Programme du travail d'Emploi et Développement social Canada</td><td></td></tr>
<tr><td>Langue de communication future dans le cadre du processus d'approvisionnement – veuillez indiquer le français ou l'anglais</td><td colspan="3"></td></tr>
<tr><td>Province ou territoire canadien visé par la demande selon les lois en vigueur</td><td colspan="3"></td></tr>
</table>

Niveau de cote de sécurité du répondant Le nom dans l'attestation de sécurité doit correspondre à la dénomination sociale du répondant. Si ce n'est pas le cas, la cote de sécurité n'est pas valide pour le répondant.	Cote de sécurité	
	Date d'attribution	
	Entité émettrice (TPSGC, GRC, etc.)	
	Dénomination sociale de l'entité à qui la cote de sécurité a été attribuée	

En apposant ma signature ci-dessous, je confirme, au nom du répondant, que j'ai lu l'invitation à se qualifier en entier, y compris les documents intégrés par renvoi. J'atteste également ceci : 1. Le répondant considère qu'il possède les compétences et qu'il offre des produits répondant aux exigences obligatoires décrites dans l'IQ; 2. Tous les renseignements fournis sont exacts et complets; 3. Le répondant accepte de se conformer à toutes les modalités et conditions de la présente IQ, documents intégrés par renvoi compris.
Respondent Authorization: Représentant autorisé du répondant
Nom:
Adress:
Courriel:
Signature du représentant autorisé du répondant :
Téléphone:
Date:
Si le répondant fournit une réponse à l'ISQ à titre de coentreprise, il doit en indiquer la dénomination sociale complète, l'adresse et le numéro d'entreprise – approvisionnement (le cas échant) de la coentreprise. [Le répondant ajoutera des lignes si la coentreprise compte plus de deux membres].
Nom:
Adress:
Courriel:
Signature du représentant autorisé du répondant :
Téléphone:
Date:

ébauche

Annexe E : Processus d'approvisionnement agile et collaboratif

1.1 Introduction

a) Le Canada adopte une approche agile et collaborative relative au processus d'approvisionnement pour le projet CD-DAR en réunissant le gouvernement et l'industrie pour concevoir et améliorer l'approvisionnement de façon itérative afin d'obtenir des résultats.

b) La phase d'ISQ du projet CD-DAR ainsi que la phase de diligence raisonnable continueront de suivre un processus d'approvisionnement agile et collaboratif qui facilite un dialogue solide et une communication bilatérale, une rétroaction de qualité et la divulgation de renseignements jusqu'à la publication de la DP.

c) Le Canada reconnaît que la consultation et la collaboration tout au long d'un processus d'approvisionnement peuvent aider à réduire le fardeau global du retravail des soumissionnaires potentiels et aider les fournisseurs à obtenir un rendement raisonnable de leurs investissements, et que le processus global offre de généreuses retombées aux Canadiens.

1.2 Avant cette ISQ

a) Avant l'ISQ, le processus de collaboration au sein de l'industrie a commencé par la publication de lettres d'intérêt (LI) sur le site Achats et ventes en décembre 2016 pour les projets de sensibilisation à la cybersécurité (SC) et de cyberopérations défensives - aide à la décision (CD-AD) pour déterminer si une solution existante était disponible sur le marché. Les résultats des LI indiquaient qu'il n'existait pas de solution disponible dans le commerce, mais ils démontraient que l'industrie souhaitait vivement collaborer avec le MDN et les FAC pour répondre à ses besoins. Comme les résultats de la LI n'ont pas fourni suffisamment d'information au MDN pour faire avancer le projet, il a été déterminé qu'une demande de renseignements plus détaillée était nécessaire. Les numéros de dossier de CD-AD et de SC sont indiqués ci-dessous. Bien qu'ils soient maintenant inactifs, les deux sont accessibles sur le site Achats et ventes.

LI de CD-AD

Numéro de référence sur le site Achats et ventes : PW-$$QE-049-26100
Numéro de la demande de soumissions : W6369-17DE25/A

LI de SC

Numéro de référence sur le site Achats et ventes : PW-$$QE-049-26099
Numéro de la demande de soumissions : W6369-17DE26/A

b) Une DDR a été publiée en décembre 2017 sur le site achatsetventes.gc.ca dans le cadre du projet de CD-AD et a fourni davantage de renseignements sur le projet à l'industrie et a sollicité des commentaires détaillés de l'industrie sur les exigences opérationnelles et techniques, les coûts, et le calendrier.

DDR de CD-AD

Numéro de référence sur le site Achats et ventes : PW-$$QE-049-26594
Numéro de la demande de soumissions : W6369-17DE25/B

ébauche

c) Une journée de l'industrie non classifiée a été tenue en février 2018 pour présenter à l'industrie un aperçu des exigences et du processus de consultation prévu, et solliciter les commentaires de l'industrie. Les questions posées et les réponses données, et les commentaires découlant de ce dialogue avec les participants ont été affichés sur le site Achats et ventes.

d) À la suite de la journée de l'industrie, des réunions individuelles classifiées ont eu lieu en mars 2018 pour présenter et discuter l'annexe classifiée de la DDR de CD-AD. Tous les fournisseurs ont été invités à présenter une demande de réunion individuelle, les seuls critères étant qu'ils répondaient aux exigences de sécurité détaillées dans la DDR. Les questions et réponses classifiées ont été distribuées sur demande aux fournisseurs qui ont assisté aux réunions ou qui ont satisfait aux exigences de sécurité et ont demandé une copie dans les délais précisés dans la DDR. Toutes les questions et réponses non classifiées provenant des réunions individuelles ont été affichées sur le site Achats et ventes.

1.3 Pendant la phase d'ISQ

a) Ébauche de l'ISQ : Une ébauche de l'ISQ sera affichée sur le site Achats et ventes, ce qui permettra à l'industrie de fournir des commentaires avant l'émission de l'ISQ finale. Les fournisseurs seront invités à formuler des commentaires et à poser des questions par écrit sur l'ébauche de l'ISQ. Les réponses seront affichées sur le site Achats et ventes.

b) ISQ officielle : L'ISQ officielle sera affichée sur le site Achats et ventes. Il s'agit de la première étape du processus de qualification pour être admissible à soumissionner pour la DP dans le cadre du projet CD-DAR.

c) Les répondants devront soumettre leurs réponses avant l'heure et la date indiquées dans l'ISQ.

d) Le gouvernement du Canada (GC) informera les fournisseurs des résultats de l'évaluation.

1.4 Pendant la phase de diligence raisonnable

a) Le GC a l'intention de publier une ébauche complète de la DP, qui comprend un élément classifié, à l'intention des fournisseurs préqualifiés.

b) Afin de tenir l'ensemble de l'industrie informée des exigences, le GC affichera les éléments non classifiés de l'ébauche de la DP sur le site Achats et ventes au moyen d'une demande de renseignements (DDR).

c) Afin d'obtenir des commentaires sur l'ébauche de la DP, le GC peut organiser une conférence des soumissionnaires classifiée et des réunions individuelles classifiées avec des fournisseurs préqualifiés.

d) Le cas échéant, le GC fournira de la rétroaction sur la façon dont il utilise ou non les commentaires reçus.

e) Le GC peut apporter des modifications aux exigences et aux modalités de la DP en fonction des commentaires de l'industrie.

ébauche

f) Dans la mesure du possible, tout au long du processus, le GC prévoit répondre et publier les questions et réponses soumises par d'autres fournisseurs (et non par des fournisseurs préqualifiés) sur le site Achats et ventes.

g) Dans la mesure du possible, tout au long du processus, on répondra aux questions non classifiées posées par des fournisseurs préqualifiés et on les affichera sur le site Achats et ventes.

h) Les questions et réponses classifiées ne seront fournies qu'aux fournisseurs préqualifiés qui satisfont aux exigences de sécurité requises.

j) Le GC prévoit publier les questions posées et les réponses données, dans la mesure du possible, tout au long du processus.

1.5 Demande de propositions (DP)

a) Le GC fournira la DP complète, qui comprend des éléments classifiés, aux fournisseurs préqualifiés et invitera les fournisseurs préqualifiés à soumissionner sur la demande.

b) Pour tenir l'ensemble de l'industrie informée, le GC affichera les éléments non classifiés de la DP sur le site Achats et ventes, mais seuls les fournisseurs préqualifiés seront invités à soumissionner sur la demande.

ébauche

ANNEXE B – ÉBAUCHE DE DP NON CLASSIFIÉE

Pour informer l’industrie, les parties non classifiées de l’ébauche de DP seront jointes en tant que modification à cette DR lorsque l’ébauche de DP sera publiée à l’intention des fournisseurs qualifiés au terme de l’ISQ.

ANNEXE C – DP NON CLASSIFIÉE

Pour informer l’industrie, les parties non classifiées de la DP seront jointes en tant que modification à cette DR lorsque la DP sera publiée à l’intention des fournisseurs qualifiés au terme de l’ISQ.