RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
See Above

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires

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

Issuing Office - Bureau de distribution
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

Title - Sujet Defensive Cyber Operations	
Solicitation No. - N° de l'invitation W6369-17DE25/B	**Amendment No. - N° modif.** 003
Client Reference No. - N° de référence du client W6369-17DE25	**Date** 2018-02-28
GETS Reference No. - N° de référence de SEAG PW-$$QE-049-26594	
File No. - N° de dossier 049qe.W6369-17DE25	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-06-05**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Wight, Patti	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone (819) 420-1757 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** See Herein	

Instructions: See Herein

Instructions: Voir aux présentes

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

National Defence Défense nationale

Instructions administratives

LCol Yves Turcotte, Officier d’état-major sénior, Développement et élaboration des besoins de la capacité cybernétique

Canada

1. Rappel sur les consignes de sécurité du bâtiment;
2. Cabinet d’aisance, l’Espace Fumeur et la Zone de Pause; et
3. Questions.

Consignes de sécurité

1. Les visiteurs sont priés de demeurer dans les zones du Mess pour les non-membres; et
2. Les sorties d’urgences sont situées sur le parterre à votre gauche et à votre droite.

Cabinet d’aisance

Les cabinets d’aisance pour hommes et femmes sont situés à l’extérieur de la sale à votre droite.

Espace Fumeur

L’Espace Fumeur est situé à l’extérieur du bâtiment.

Zone de Pause

Une pause aura lieu à 10:00 à l’entrée de cette salle.

Questions?

Cyberopérations défensives - Aide à la décision (CD-AD)
et
Sensibilisation à la cybersécurité (SC)

SÉANCE DE CONSULTATION DE L'INDUSTRIE

Ottawa, Ontario

Le 26 février 26

Services publics et Approvisionnement Canada
Public Services and Procurement Canada
Canada

ALLOCUTION D'OUVERTURE

Cmdre R. Feltham

Directeur général de la
Cyberdéfense

ALLOCUTION D'OUVERTURE

Jeff Waring

Directeur général

Innovation, Sciences et Développement économique Canada (ISDE)

ALLOCUTION D'OUVERTURE

Al Hamel

Directeur général / Intérimaire

Secteur de l'approvisionnement et du soutien en équipement aérospatial et terrestre (SASEAT)

Direction générale des approvisionnements, SPAC

Al Hamel

A/Director General

- Biographical Sketch - Al Hamel, Col (Ret'd), CD, PEng

- A native of Coleville, Saskatchewan, Al Hamel started his academic and military career at Royal Roads Military College in Victoria, B.C. in 1970. Graduating from the Royal Military College of Canada in Kingston in 1974, and then trained as a military Communications and Electronics Engineering officer, Al set out on a 31-year adventure that included jobs such as Telecommunications Maintenance Officer at Canadian Forces Station Sioux Lookout in north-western Ontario, Regimental Signals Officer with the Royal Canadian Dragoons in Lahr, Germany, Commandant of the Canadian Forces School of Communications and Electronics in Kingston and Commander of the multinational, Signal Support Group at NATO's SFOR HQ in Sarajevo, not to mention a number of notable engineering and project management postings at Land Force Headquarters, St. Hubert and National Defence Headquarters in Ottawa. Al's last military appointment was as Director, Land Command Systems Program Management.

- Upon retiring from the Canadian Forces in April 2006, Al accepted a Public Service appointment with the Department of Public Works and Government Services Canada. After working for 4 ½ years in the IT Services Branch of PWGSC he joined Acquisitions Branch in October 2010, and he has been Senior Director, Electronics, Munitions and Tactical Systems Procurement since that time. He is also currently Acting Director-General, Land and Aerospace Equipment Procurement and Support Sector.

- Al holds a Bachelor's Degree in Electrical Engineering and a Master's Degree in Computer Engineering, both from the Royal Military College of Canada. He has been a Professional Engineer licensed to practice in the province of Ontario since 1976.

Le mandat de SPAC

- Services publics et Approvisionnement Canada agit à titre d'organisme de services communs pour le gouvernement du Canada

- Ses activités visent surtout à offrir aux autres ministères, conseils et organismes des services à l'appui de leurs programmes

- Les services offerts visent :
  - Biens immobiliers
  - La comptabilité et gestion bancaire
  - Receveur general
  - Informatiques et en télécommunications
  - Les contrats et les achats (ce sur quoi l'exposé portera principalement)

Objectifs et principes de passation de contrats

- Intégrité
- Concurrence
- Ouverture et transparence
- Appui aux ministères et organismes pour atteindre leurs objectifs
- Objectifs socio-économiques
- Cadre juridique et politique, y compris les accords commerciaux

Achats de matériel de défense – quel est notre rôle?

- En vertu de la *Loi sur la production de défense* (1951), le ministre de TPSGC a le **pouvoir exclusif** de faire l'acquisition du matériel (fournitures) de défense

- Établir et gérer des contrats dans le but d'acquérir un vaste éventail de systèmes techniques complexes pour l'armée, la marine et la force aérienne, y compris l'acquisition, entre autres :
  - d'avions et de systèmes militaires et civils
  - de systèmes de navire et de marine
  - de systèmes d'armement et de munitions
  - de véhicules blindés
  - de systèmes électroniques et de communication
  - de dispositifs d'entraînement et de simulateurs
  - d'activités connexes de réparation et de remise en état
  - de services de sécurité et de guerre électronique

- Nous gérons les achats conformément au Programme d'approvisionnement en munitions afin de maintenir la capacité de l'industrie canadienne dans le domaine des munitions

Intervenants en matière d'achats de matériel de défense au Canada

Innovation, Sciences et Développement économique Canada

SPAC

Conseil du Trésor

Bureau du Conseil privé (BCP)

MDN

Finance

Justice

Agences de développement régional

Industrie

Affaires mondiales Canada

Ordre du jour – Journée de l'industrie

Allocution d'ouverture - Directeur général Cyberdéfense	MDN
Allocution d'ouverture - Directeur général	ISDE
Allocution d'ouverture - Directeur général SASEAT	SPAC
Processus de consultation de l'industrie	SPAC
Règles d'engagement	SPAC
Processus de demande d'attestation de sécurité d'installation/d'inscription au Programme des marchandises contrôlées	SPAC
Retombées industrielles et technologiques	ISDE
Aperçu des besoins opérationnels	MDN
Questions et réponses	tout
Mot de clôture	SPAC

Processus de consultation de l'industrie

Patti Wight
Spécialiste en approvisionnements
Direction générale des approvisionnements,
SPAC

Consultation de l’industrie

- Le Canada prévoit consulter activement l'industrie pendant tout le processus d'approvisionnement pour assurer une fin de projet réussie.
- Le processus de demande de renseignements (DDR) et d’engagement offre à l'industrie l'occasion de présenter ses capacités et ses points de vue concernant les exigences du Canada relativement au projet Defensive Cyber Operations - Decision Support (DCO-DS) et au projet de sensibilisation à la sécurité.
- Le Canada peut utiliser les informations recueillies pour l'élaboration d'une demande de propositions (DP).

Principes directeurs de consultation de l'industrie

Transparence : assurer l'intégrité du processus d'approvisionnement en communiquant aux intervenants toutes les activités et tous les documents liés à l'approvisionnement;

Équité : tous les intervenants auront une chance égale d'accéder aux activités de consultation;

Rapidité : les activités de consultation sont prévues et se dérouleront tôt dans le processus d'approvisionnement;

Pertinence : inclure des résultats concrets, utiles et actuels qui sont conformes aux priorités du gouvernement du Canada.

Processus de consultation et d'approvisionnement proposé

- **L'étape 1: hiver 2016 à l'automne 2019**
  - **Lettre d'intérêt :** Une lettre d'intérêt (LI) initiale réunissant les deux projets a été publiée en décembre 2016 et sa date de clôture était en janvier 2017.
  - **Demande de renseignements :** La présente DR vise à fournir des renseignements plus détaillés à l'industrie et servira de point permanent et unique pour les communications officielles sur le projet. Elle a surtout pour but de solliciter des commentaires détaillés de l'industrie sur les exigences opérationnelles et techniques, les coûts et le calendrier.
  - **Journée de l'industrie non classifiée :** Présenter un aperçu des exigences et du processus de consultation.
  - **Rencontres individuelles :** Les rencontres individuelles classifiées visent à distribuer et à présenter l'annexe classifiée de la DR, ainsi qu'à en discuter.
  - **Réunion de suivi en groupe :** Les réunions de suivi en groupe classifiées visent à distribuer les questions et réponses classifiées.

Processus de consultation et d'approvisionnement proposé

- **Étape 2: Automne 2019**
  - **Request for Demande de renseignements :** La DR publiée à l'étape 1 demeurera ouverte afin de fournir des directives et une assistance aux fournisseurs pour qu'ils obtiennent l'attestation de sécurité requise.
  - **Demande de propositions préliminaire :** La version préliminaire d'une DP pour chaque projet ou un seul projet combiné peut être présentée aux fournisseurs qui satisfont aux exigences de sécurité aux fins d'examen et de commentaires.
- **Étape 3: Été/automne 2020**
  - **Demande de propositions :** La demande de propositions officielle pour chaque projet ou un seul projet combiné sera publiée.
  - **Évaluation :** Les soumissions seront évaluées conformément aux modalités de la DP.
- **Étape 4: Été 2021**
  - **Attribution du contrat :** Le contrat sera attribué au soumissionnaire retenu conformément aux modalités de la DP.

Consultation de l'industrie terminée

Lettre d'intérêt (LI)

Une lettre d'intérêt (LI) initiale réunissant les deux projets a été publiée en décembre 2016 et sa date de clôture était en janvier 2017. La LI a permis d'informer l'industrie, à un haut niveau, des projets et a cherché à obtenir des commentaires généraux sur les solutions possibles et les coûts. Elle a avisé les fournisseurs potentiels que la Politique des RIT peut être appliquée.

Principales constatations

- Il existe des technologies permettant d'offrir des solutions rapidement et de façon rentable.
- L'industrie est prête à assumer le rôle de principal intégrateur de systèmes, d'intégrateur de systèmes subalterne ou de fournisseur de produits.
- L'industrie a signalé l'étroite corrélation entre les deux projets et le besoin de les envisager conjointement, sous forme d'un seul projet.
- L'industrie a indiqué que d'autres détails devront être fournis dans le cadre de l'exercice de justification des prix.
- Des séances de consultation individuelles devront être tenues en vue de fournir aux fournisseurs détenant une attestation SECRET les renseignements classifiés justifiant une analyse détaillée.

DR les principaux objectifs de la DR

La présente DR est publiée avec les principaux objectifs suivants :

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

Principales étapes de la DDR actuelle

- **Séance de consultation en groupe de l'industrie – le 26 février 2018**
  - Journée de l'industrie « non classifiée » s'adressant à tous les répondants intéressés de l'industrie.
  - Présenter à l'industrie un aperçu du processus d'approvisionnement, l'approche de consultation, les exigences relatives à la sécurité et un aperçu « non classifié » des projets.
  - Présenter les règles d'engagement du processus d'approvisionnement – **Annexe G de la DDR.**
  - Permettre à l'industrie de poser des questions et d'obtenir des renseignements en vue de bien comprendre le besoin.
- **Rencontres individuelles « classifiées » – du 26 février 2018 au 2 mars 2018**
  - Présenter aux fournisseurs détenant une attestation de sécurité un aperçu de l'Annexe C, qui comporte des renseignements classifiés.
  - Fournir aux fournisseurs détenant une attestation de sécurité une copie papier de l'Annexe C. À noter que l'Annexe C sera fournie uniquement en personne.
  - Inviter les fournisseurs à discuter et à fournir des commentaires uniquement en lien avec l'Annexe C.
  - Une rencontre de suivi « classifiée » en groupe pourra avoir lieu, au besoin, pour distribuer les questions et les réponses portant sur les renseignements classifiés.
- **Soumissions présentées en réponse à la DDR – le 23 mars 2018**
  - Les fournisseurs sont priés de répondre à la DDR actuelle d'ici le 23 mars 2018.
  - Tous les fournisseurs intéressés peuvent présenter des réponses formelles aux questions posées dans la DDR.

Règles d'engagement

Christine Picknell

Spécialiste en approvisionnements

Direction générale des approvisionnements, SPAC

Règles et principes généraux

Ces règles d'engagement s'appliquent à l'ensemble du processus d'engagement.

- Un des principes fondamentaux de l'engagement de l'industrie est que le processus soit réalisé avec le plus haut degré de justice et d'équité entre toutes les parties. Nulle personne ou organisation ne doit recevoir ni sembler avoir reçu un quelconque avantage inhabituel ou injuste par rapport aux autres.
- Les présentes règles d'engagement précoce entreront en vigueur à la signature de ce document, et prendront fin au moment de la publication de la demande de propositions.
- Le processus d'engagement comprendra la demande de renseignement, les rencontres individuelles, une éventuelle ébauche de DP et tout autre processus jugé nécessaire par le responsable de l'approvisionnement.
- Afin de maximiser les avantages du processus d'engagement, le Canada peut s'efforcer de solliciter les commentaires des participants sur diverses questions soulevées.
- Les rencontres individuelles ne sont disponibles que pour les participants qui satisfont aux exigences de sécurité.
- Les informations classifiées ne peuvent être divulguées qu'aux participants qui satisfont aux exigences de sécurité.

Règles et principes généraux

- Les solutions, les idées ou les questions soulevées au cours des rencontres individuelles feront l'objet d'un examen plus poussé par le Canada.
- Une version préliminaire de la DP pour examen définitif avant la publication officielle de la DP peut être mise à la disposition des participants qui satisfont aux exigences de sécurité.
- Le Canada ne divulguera pas de renseignements exclusifs ou délicats sur le plan commercial concernant un participant à d'autres participants ou à des tiers, sauf dans la mesure où la loi l'exige.
- Les répondants éventuels sont informés que tout renseignement soumis au Canada dans le processus d'engagement peut être utilisé par le Canada dans l'élaboration d'une demande de propositions concurrentielle

Modalités

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

- Les participants doivent exposer leurs points de vue quant à l'approvisionnement et fournir des solutions positives aux problèmes soulevés. Tous les participants intéressés qui satisfont aux exigences de sécurité auront les mêmes chances de partager leurs idées et leurs suggestions.
- Aucun enregistrement audio ou visuel ne sera autorisé pendant les rencontres individuelles.
- Les participants doivent prévenir le Canada s'ils prévoient être accompagnés d'un avocat au moment de la rencontre individuelle. Le Canada se réserve le droit de refuser toute réunion en présence d'un avocat.
- Les participants NE révéleront PAS ou ne discuteront d'aucune information sur les MÉDIAS ou dans les JOURNAUX quant à cette exigence au cours du processus d'engagement. Si les participants sont interrogés par les médias, ils doivent les orienter vers le Bureau des relations avec les médias de SPAC au 819-956-2313.
- Les participants doivent présenter leurs questions et leurs commentaires UNIQUEMENT à l'autorité contractante de SPAC ou aux représentants autorisés du Canada, conformément aux indications données par l'autorité contractante. Toute communication avec des représentants non autorisés du Canada peut faire l'objet d'une divulgation complète par le Canada sur Achatsetventes.gc.ca.

Modalités

- Les médias ne peuvent participer au processus. Les médias doivent présenter leurs questions au Bureau des relations avec les médias de SPAC.
- Le Canada n'est pas tenu d'émettre une DP ou de négocier un contrat pour les projets.
- S'il publie une DP, le Canada doit en établir, à son gré, toutes les modalités.
- Le Canada ne remboursera aucune personne ou entité pour tout coût engagé pour la participation à ce processus d'engagement de l'industrie.
- La participation n'est pas obligatoire. Ne pas participer à ce processus n'empêche pas le soumissionnaire de soumettre une proposition lorsque la DP finale sera publiée.
- La documentation préliminaire (DP, plan d'évaluation, EDT) sera diffusée aux participants qui satisfont aux exigences de sécurité pour obtenir leurs commentaires.
- Les lobbyistes ne seront pas autorisés à participer au processus.
- Dans le cadre de discussions informelles et de négociations de bonne foi, SPAC et le participant doivent faire tous les efforts raisonnables pour résoudre tout différend, toute controverse ou toute réclamation découlant de cet engagement de l'industrie, ou qui sont liés d'une quelconque façon à celui-ci.

Respect ♣ Intégrité ♣ Excellence ♣ Leadership

Au service du GOUVERNEMENT, au service des CANADIENS.

PROJET DE CYBER SÉCURITÉ
EXIGENCES DE SÉCURITÉ À TRAVERS LE PROGRAMME DE SÉCURITÉ DES CONTRATS



Direction générale des politiques, de la planification et de la sécurité, Secteur de la sécurité industrielle
Division de la sensibilisation 2018

Gouvernement du Canada Government of Canada

Canada

Survol

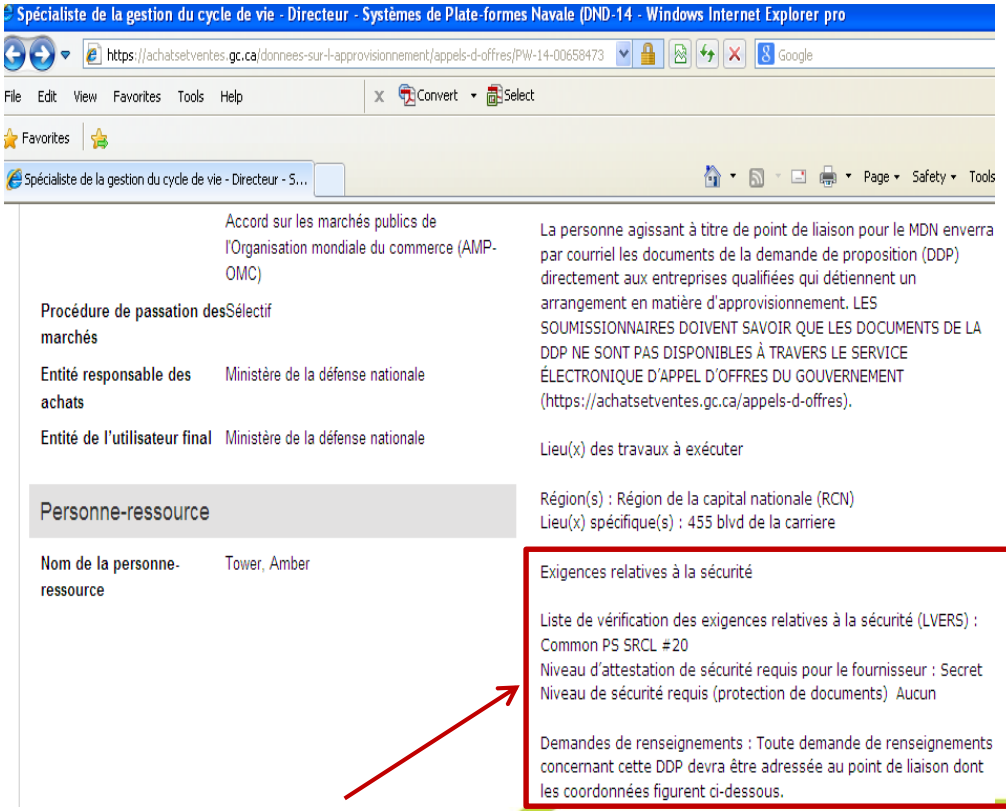
- Exigences dans les demandes de soumissions
- Le Programme de sécurité des contrats et l'inscription
  - Enquête de sécurité sur les organisations
  - Autorisation de détenir des renseignements
  - Autorisation de traiter les technologies de l'information
  - Sous-traitance
- Votre rôle
- Webinaires
- Contactez-nous
- Liens utiles

Exigences dans les demandes de soumissions

Les exigences en matière de sécurité peuvent être consultées dans :

- La description de l'appel d'offres
- Les documents d'invitation à soumissionner
  - Ex. : Consulter la table des matières pour les exigences en matière de sécurité (celles-ci se retrouvent généralement à la Partie 7 – Clauses du contrat subséquent et la LVERS est généralement joint en annexe)

https://achatsetventes.gc.ca/



Programme de sécurité des contrats

- Permettre à l'industrie d'obtenir des contrats de nature délicate du gouvernement au Canada et à l'étranger.
- Effectuer des enquêtes de sécurité sur des organisations et leurs employés.
- Assurer que les clauses de sécurité qui doivent être ajoutées aux contrats sont incluses aux outils de passation de contrats.
- Assurer que l'industrie se conforme aux exigences de sécurité en matière de passation de contrats.

Comment puis-je m’enregistrer au PSC?

Une **source approuvée** reconnue par le gouvernement du Canada doit parrainer votre organisation.

- La source approuvée doit présenter une demande d’Enquête de sécurité sur une organisation du secteur privé (**ESOSP**) et, si applicable, une Liste de vérification des exigences relatives à la sécurité (**LVERS**) pour votre organisation.
- L’ESOSP déterminera le type d’enquête de sécurité nécessaire.

Qui est une source approuvée reconnue par le PSC?

- Un agent d'approvisionnement du gouvernement – un agent qui effectue des achats spécialisés préalables de biens et de services;
- Un agent de sécurité ou un gestionnaire de projet du gouvernement du Canada chargé du projet pour lequel vous avez présenté une soumission ou comptez en présenter une;
- Un entrepreneur principal inscrit au PSC pour lequel vous faites de la sous-traitance (contrats de sous-traitance approuvés seulement); ou
- Les administrations nationales et désignées de la sécurité, au nom d'une entreprise ou d'un gouvernement étranger qui octroie un contrat à votre organisation.

Type d’enquête de sécurité

	Renseignements et biens	Enquête sur les organisations	Enquête de sécurité sur le personnel
CLASSIFIÉ Intérêt national	Très secret	Attestation de sécurité d’installations (ASI)	Très secret
	Secret		Secret
	Confidentiel		
PROTÉGÉ Non lié à l’intérêt national	Protégé C	Vérification d’organisation désignée (VOD)	CF – Approfondi
	Protégé B		Cote de fiabilité (CF)
	Protégé A		

Enquête de sécurité sur les organisations

À la réception d'une demande valide d'ESOSP provenant d'une source approuvée, le **PSC contactera votre organisation** par courriel ou par la poste afin de demander l'information requise pour débuter le processus d'enregistrement.

Le PSC exigera l'information suivante :

- la structure, la propriété et le statut juridique de votre organisation;
- la nomination d'un agent de sécurité d'entreprise (ASE) et/ou d'un agent de sécurité d'entreprise remplaçant (ASER);
- les noms des cadres supérieurs clés (CSC) (s'il y a accès à des renseignements/biens confidentiels, secrets ou très secrets);
- formulaires et documents d'enquête de sécurité sur le personnel pour les ASE, ASER et/ou les CSC.

Autorisation de détenir des renseignements

- Si la DI, la DP ou le contrat nécessite la **protection de renseignements ou de biens de nature délicate dans votre ou vos installations**, votre organisation devra également obtenir une autorisation de détenir des renseignements (ADR) au niveau spécifié dans l'avis d'appel d'offre ou du contrat.

- Le PSC effectue des inspections de la sécurité physique, **avant l'attribution du contrat**, lorsque les exigences en matière de sécurité contractuelle suivantes ont été identifiés:

  - Autorisation de détenir des renseignements
  - Autorisation de traiter les technologies de l'information

Autorisation de traiter les technologies de l’information

- Si votre organisation est **tenue d’utiliser ses systèmes de TI pour accéder, produire, traiter ou stocker électroniquement des renseignements protégés ou classifiés dans le cadre de contrats conclus avec le gouvernement**, elle devra également obtenir une autorisation de traiter les TI au niveau spécifié dans l’avis d’appel d’offre ou le contrat.

- Les exigences en matière de TI sont définies dans le document technique joint au contrat.

- Une inspection de sécurité informatique pour les exigences de sécurité des contrats TI doit être effectuée, typiquement **après l’attribution du contrat**.

- L'inspection informatique examine tous les atouts informatiques utilisés pour créer le livrable du contrat.

Délais de traitement

Enquête de sécurité sur les organisations	Délais de traitement prévus
Vérification d'organisation désignée	Trois mois ou plus
Attestation de sécurité d'installations (secret)	Six mois ou plus
Attestation de sécurité d'installations (très secret)	Douze mois ou plus
Autorisation de détenir des renseignements	Varie
Autorisation de traiter les technologies de l'information (TI)	Varie

Normes de service

Enquête de sécurité sur le personnel	Normes de service du PSC
Cote de fiabilité (simple)	7 jours ouvrables
Cote de fiabilité (complexe*)	Jusqu'à 120 jours ouvrables
Secret (simple)	Jusqu'à 4 mois
Secret (complexe*)	Jusqu'à 12 mois
Très Secret	12 mois +

* Information et/ou vérification additionnelle à traiter

Sous-traitance

Les contrats de sous-traitance sont utilisés par les entrepreneurs principaux qui souhaitent sous-traiter une partie du contrat principal à une autre organisation ou à un travailleur autonome.

L'organisation qui a l'intention de sous-traiter est responsable de:

1. remplir une LVERS pour déterminer les exigences de sécurité du contrat de sous-traitance;
2. demander une enquête de sécurité sur une organisation du secteur privé (ESOSP) au nom du sous-traitant;
3. présenter la LVERS et le formulaire d'ESOSP au PSC pour approbation;
4. obtenir les clauses de sécurité et la LVERS et les insérer dans le contrat de sous-traitance;
5. confirmer que l'organisation et le personnel du sous-traitant détiennent les attestations appropriées;
6. soumettre au PSC une copie du contrat de sous-traitance octroyé contenant la LVERS.

Les travaux ne peuvent pas être entrepris tant que le sous-traitant n'a pas obtenu les attestations de sécurité appropriées.

Étape 1

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

Étape 2

Étape 2	
Demande de propositions préliminaire*	Protection des documents : SECRET
Consulter l'information classifiée	Personnel : SECRET, réservé aux Canadiens
Obtenir une version imprimée de l'information classifiée	Attestation de sécurité d'installation : SECRET, réservé aux Canadiens Membres du personnel qui transportent les documents : SECRET, réservé aux Canadiens Protection des documents : SECRET
Assister aux rencontres classifiées	Personnel : SECRET, réservé aux Canadiens

Étape 3

Étape 3	
Demande de propositions*	Attestation de sécurité d'installation : SECRET, réservé aux Canadiens
	Personnel : SECRET, réservé aux Canadiens Protection des documents : SECRET
Consulter l'information classifiée	Personnel : SECRET, réservé aux Canadiens
Obtenir une version imprimée de l'information classifiée	Attestation de sécurité d'installation : SECRET, réservé aux Canadiens Membres du personnel qui transportent les documents : SECRET, réservé aux Canadiens Protection des documents : SECRET
Assister aux rencontres classifiées	Personnel : SECRET, réservé aux Canadiens

Étape 4

Étape 4	
Contrat*	Attestation de sécurité d'installation : TRÈS SECRET, réservé aux Canadiens Personnel : TRÈS SECRET SIGINT, réservé aux Canadiens* Protection des documents : SECRET, OTAN SECRET

Votre rôle

- Trouver une source approuvée.
- Respecter le processus d’enregistrement du PSC.
- Obtenir et maintenir une attestation de sécurité d’organisation.
- Filtrer le personnel concerné par le contrat de nature délicate du gouvernement du Canada.
- Respecter les exigences de sécurité physique et de TI si nécessaire.
- Identifier les sous-traitants et veiller à ce que les contrats de sous-traitance respectent les exigences de sécurité.

Webinaires

- Comment obtenir une attestation de sécurité auprès du Programme de sécurité des contrats
- Autorisation de détenir des renseignements
- Passation de marchés à l’étranger
- Manipulation et sauvegarde des renseignements et des biens de nature délicate
- Sous-traitance
- Compléter une demande de vérification d’organisation désignée
- Compléter une demande d’attestation de sécurité d’installations

Demander une copie de l'enregistrement:
SSIDSICSensibilisation.ISSCISDOutreach@tpsgc-pwgsc.gc.ca

Contactez-nous

Renseignements généraux

Téléphone
Sans frais : 1-866-368-4646
Région de la capitale nationale : 613-948-4176

Courriel
ssi-iss@tpsgc-pwgsc.gc.ca

Site internet
https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html

Liens utiles

Personnes-ressources responsables des numéros d'identification des biens et services pour TPSGC
https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/numero-d-identification-des-biens-et-services/personnes-ressources-responsables-des-nibs

Ressources liées à la sécurité des contrats
http://www.tpsgc-pwgsc.gc.ca/esc-src/ressources-resources-fra.html

Formulaires du Programme de sécurité des contrats
http://ssi-iss.tpsgc-pwgsc.gc.ca/formulaires-forms/index-fra.html

Vidéo – Dactylotechnie électronique (prise d'empreintes digitales)
http://www.tpsgc-pwgsc.gc.ca/esc-src/formation-training-fra.html#s3

Merci!

Annex

Project Screening Requirements

Project Stage	Description of Project Stage	Level of Personnel Clearance and Document Safeguarding (e.g. Reliability, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
1	Industry Engagement Stage supporting Options Analysis Phase	• SECRET for Personnel Assigned, and • SECRET for Document Safeguarding	• Reviewers of Annex C of RFI during Options Analysis Phase	Classified Meeting Room for One-on-One Industry Engagement Meeting / SECRET	Canadian, UK, USA, Australia
2	Industry Engagement Stage supporting Definition Phase	• SECRET for Personnel Assigned, and • SECRET for Document Safeguarding	• Reviewers of Classified Annexes of RFI	Classified Meeting Room for One-on-One Industry Engagement Meeting / SECRET	Canadian
3	Solicitation Stage supporting Definition and/or Implementation Phase	• SECRET for Personnel Assigned, and • SECRET for Document Safeguarding	• Reviewers of Classified Annexes of RFP	Classified Meeting Room for One-on-One Industry Engagement Meeting / SECRET	Canadian

Project Screening Requirements

Project Stage	Description of Project Stage	Level of Personnel Clearance and Document Safeguarding (e.g. Reliability, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
4	Contract Award Stage during Implementation Phase	• TOP SECRET (SIGINT) for Personnel Assigned, and • SECRET and NATO SECRET for Document Safeguarding	• Project Manager, • Senior Business Systems Analyst, • Senior Systems Engineer/Developer, • Field Service Representatives, and • Equivalent tasked Subcontractors	High Security Zones within DND / TOP SECRET (SIGINT)	Canadian
		• NATO SECRET and SECRET for Personnel Assigned, and • NATO SECRET and SECRET for Document Safeguarding	• Intermediate Engineer/Developer, • Junior Engineer/Developer, and • Equivalent tasked Subcontractors	Security Zones within DND / NATO SECRET and SECRET	Canadian
		• Enhanced Reliability for Personnel Assigned, and • No Requirement for Document Safeguarding	• Administrative Staff	No Site Access / UNCLASSIFIED	Nil

Droits d'auteur

Programme des marchandises contrôlées

Journée d'industrie pour le Projet d'aide à la décision pour les cyberopérations défensives
le 26 février 2018

Dominic Dubé

Chef, Gestion de programmes et apprentissage
Programme des marchandises contrôlées

Services publics et Approvisionnement Canada (SPAC)

Le Programme des marchandises contrôlées

- Créé en 2001 à l'appui de la prestation de l'exemption canadienne en vertu de l'*International Traffic in Arms Regulations* (ITAR) des États-Unis .

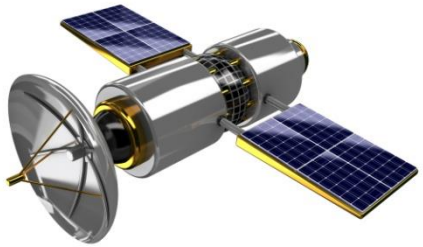
- Prescrit par la *Loi sur la production de défense* (LPD) et le *Règlement sur les marchandises contrôlées* (RMC)

Raison d'être pour le Programme des marchandises contrôlées

« Pour s'assurer que les marchandises contrôlées sont protégés pendant la possession des entreprises du secteur privé et protégé contre tout accès non autorisé »

Définition des marchandises contrôlées

- Les marchandises contrôlées sont principalement des marchandises qui sont sujettes aux mesures de contrôle intérieur du gouvernement du Canada et définies par la *Loi sur la production de défense*, notamment des composants et des données techniques d'une importance militaire ou servant à assurer la sécurité nationale.



En résumé, les marchandises contrôlées sont

- des marchandises, indépendamment de leur lieu de fabrication, d'une importance stratégique ou ayant des répercussions sur la sécurité nationale, notamment des composants et des technologies (par exemple des plans et des devis descriptifs sur papier ou en format électronique)

- du matériel de défense d'origine américaine qui est inscrit à la Liste de matériel de guerre des États-Unis, partie 121 de l'*International Traffic in Arms Regulations* des États-Unis (disponible en anglais seulement), compte tenu de ses modifications successives

- des marchandises, indépendamment de leur lieu de fabrication, qui sont fabriquées à partir de données techniques d'origine américaine et qui sont contrôlées par l'*International Traffic in Arms Regulations*

Liste des marchandises contrôlées

- Liste des marchandises contrôlées figurant à l'annexe (article 35) de la *Loi sur la production de défense*

- Guide de l'annexe de la *Loi sur la production de défense*
  - fournit une liste simplifiée des articles qui sont définis comme des marchandises contrôlées par la *Loi sur la production de la défense*
  - permet de déterminer si un article est inclus dans la Liste des marchandises contrôlées.
  - l'annexe a préséance sur le guide

Pourquoi s’inscrire

- C’est la loi. Les personnes et les organisations qui doivent **examiner**, **posséder** ou **transférer** des marchandises contrôlées sont tenues de s’inscrire au Programme des marchandises contrôlées. À l’inscription, les demandeurs doivent démontrer qu’ils ont besoin d’examiner, de posséder ou de transférer des marchandises contrôlées.

- Le défaut de s’inscrire peut constituer une infraction en vertu des lois fédérales et entraîner des poursuites et des sanctions.

Toute personne qui omet de se conformer à la *Loi sur la production de défense* peuvent :

- avoir leur inscription au Programme des marchandises contrôlées, suspendus ou révoqués

- faire face la poursuite pour défaut de se conformer et être assujettie à une amende maximale de 2 000 000 $, ou une peine d'emprisonnement maximale de 10 ans

Vous devez vous inscrire à titre de personne ou d'organisation avant de pouvoir :

- examiner, posséder ou transférer des marchandises ou des technologies contrôlées au Canada

- transférer des marchandises contrôlées à l'extérieur du Canada
  - il faut obligatoirement s'inscrire au programme pour obtenir une licence d'exportation d'Affaires mondiales Canada

- recevoir, dans le cadre de demandes de soumissions, des documents qui comportent des renseignements sur des marchandises ou des technologies contrôlées

Comprendre ce que signifient les termes « examiner, posséder ou transférer des marchandises contrôlées »

- **Examiner** – Signifie étudier en détail ou analyser dans le but de connaître la signification ou les caractéristiques essentielles

- **Posséder** – Signifie posséder réellement, c'est-à-dire avoir un contrôle matériel direct sur une marchandise contrôlée à un moment donné, et posséder de droit, c'est-à-dire avoir le pouvoir et l'intention à un moment donné d'exercer un contrôle sur une marchandise contrôlée, directement ou par l'entremise d'une ou de plusieurs autres personnes

- **Transférer** – Signifie disposer d'une marchandise contrôlée ou en communiquer le contenu d'une quelconque manière

Rôles dans le Programme des marchandises contrôlées

Propriétaires

- chacun des propriétaires dont la participation dans l'entreprise est de 20 % et plus des intérêts ou des actions avec droit de vote en circulation

Personne autorisée

- habituellement, le propriétaire ou un autre cadre supérieur de l'organisme ayant le pouvoir de signature

Représentant désigné

- suit la formation obligatoire pour les représentants désignés,
- effectue des évaluations de sécurité des employés, des cadres et des administrateurs
- détermine le risque de transfert de marchandises contrôlées à une personne qui n'est ni inscrite ni exemptée d'inscription et détermine dans quelle mesure il autorise cette personne à examiner, posséder ou transférer des marchandises contrôlées
- vérifie les renseignements fournie par des travailleurs temporaires, des étudiants étrangers et les visiteurs aux fins des demandes d'exemption et de soumettre les demandes d'exemption requises au PMC

Comment s’inscrire

Pour vous inscrire au Programme des marchandises contrôlées, vous devez suivre les étapes ci-après :

1. Nommer une personne autorisée
2. Nommer un représentant désigné
3. Remplir le formulaire de demande d’inscription
4. Remplir un formulaire de demande d’évaluation de sécurité pour chaque personne concernée
5. Réviser vos demandes et la documentation complémentaire
6. Présenter votre demande

Demande d'inscription

- Présenter la demande d'inscription dûment remplie
  - Section H (Attestation et consentement), est signée par la personne autorisée
- fournir une preuve du statut juridique de votre entreprise (p. ex. une copie du certificat de constitution, un permis principal d'entreprise, etc.)
- indiquez clairement une description des activités de votre organisation et le nom de la compagnie avec laquelle vous faites affaires qui impliquent les marchandises contrôlées. Si disponible, inclure un document à l'appui provenant d'une entreprise ou d'une organisation avec laquelle vous faites des affaires en lien avec des marchandises contrôlées (une lettre d'intérêt, un contrat, une demande de propositions, etc.)
- Les marchandise contrôlées énumérés dans la section D.10
  - Lors d'une soumission d'un contrat avec des marchandises contrôlées, vérifiez auprès de l'autorité de la soumission pour obtenir les numéros de la LMC et les descriptions des marchandises contrôlées

Personne autorisée et tous les propriétaires de 20% ou plus

- Présenter la demande d'évaluations de la sécurité dûment remplie
- deux pièces d'identité délivrées par le gouvernement, dont au moins une avec photo
  - une preuve de citoyenneté (par exemple un certificat de naissance, un passeport ou une carte de résident permanent)
  - une preuve de résidence (par exemple un permis de conduire ou un document officiel délivré par le gouvernement comportant l'adresse de la personne)
- un rapport de vérification du casier judiciaire au moyen des empreintes digitales ou un rapport de vérification nominale du casier judiciaire. Quand le demandeur complétera le formulaire pour la demande du rapport, s.v.p. utilisez « **secteur privé** » pour l'emploi et s'assurer que les résultats sont envoyés à la maison du demandeur, de sorte qu'ils peuvent fournir les résultats au programme.
  - si la personne a résidé à l'extérieur du Canada pendant plus de six mois consécutifs ou plus au cours des cinq dernières années, nous exigeons un vérification nominale du casier judiciaire d'une agence de police reconnue – Exemple: certificat de bonne conduite; vérification de FBI, certificat de police

Représentant(s) désigné(s)

- Présenter la demande d'évaluations de la sécurité dûment remplie
- deux pièces d'identité délivrées par le gouvernement, dont au moins une avec photo
  - une preuve de citoyenneté (par exemple un certificat de naissance, un passeport ou une carte de résident permanent)
  - une preuve de résidence (par exemple un permis de conduire ou un document officiel délivré par le gouvernement comportant l'adresse de la personne)
- un rapport de vérification du casier judiciaire au moyen des empreintes digitales. Quand le demandeur complétera le formulaire pour la demande du rapport, s.v.p. utilisez « **secteur privé** » pour l'emploi et s'assurer que les résultats sont envoyés à la maison du demandeur, de sorte qu'ils peuvent fournir les résultats au programme.

Délais de traitement

- Une fois la demande d'inscription et tous les documents à l'appui soumis, le traitement peut prendre jusqu'à 32 jours ouvrables.
- Vous pouvez vous informer de l'état de votre demande d'inscription après un délai de quatre semaines.
- Nous acceptons seulement les demande d'inscription complète.
- Si incomplète (signatures manquantes, il manque les documents à l'appui, les résultats des empreintes digitales manquante, etc.), la demande sera retournée.

Présenter votre demande

Poste et messagerie :

Programme des marchandises contrôlées
Services publics et Approvisionnement Canada (SPAC)
3e étage
2745 rue Iris
a/s de la Salle de courrier principale de SPAC
Portage III, 0B3
11 rue Laurier
Gatineau QC K1A 0S5

Courriel: dmc-cgd@tpsgc-pwgsc.gc.ca

Télécopieur : (613) 948-1722

Liste de vérification d'enregistrement

- Compagnie
  - Demande d'inscription
  - preuve du statut juridique de l'entreprise
- Personne autorisée
  - Demande d'évaluations de la sécurité
  - deux pièces d'identité délivrées par le gouvernement
  - un rapport de vérification du casier judiciaire au moyen des empreintes digitales **ou** un rapport de vérification nominale du casier judiciaire
- Tous les propriétaires de 20% ou plus
  - Demande d'évaluations de la sécurité
  - deux pièces d'identité délivrées par le gouvernement
  - un rapport de vérification du casier judiciaire au moyen des empreintes digitales **ou** un rapport de vérification nominale du casier judiciaire
- Représentant(s) désigné(s)
  - Demande d'évaluations de la sécurité
  - deux pièces d'identité délivrées par le gouvernement
  - un rapport de vérification du casier judiciaire au moyen des empreintes digitales

Questions?

Site web: http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-fra.html

Courriel: DMC-CGD@tpsgc-pwgsc.gc.ca

Numéro sans frais : 1-866-368-4646

Région de la capitale nationale : 613-948-4176

Vous pouvez nous appeler du lundi au vendredi, de 8 h à 17 h (heure de l'Est). Les services sont disponibles en français et en anglais.

Projet Sensibilisation à la cybersécurité et projet Aide à la décision pour les cyberopérations défensives

Politique des retombées industrielles et technologiques

Tirer profit des retombées économiques

Retombées économiques pour le Canada

- Le gouvernement du Canada consulte l'industrie dans le but de comprendre comment tirer le meilleur parti de ces cyberapprovisionnements afin de réaliser des avantages économiques pour le Canada.

- Le gouvernement du Canada envisage d'appliquer la Politique des **retombées industrielles et technologiques (RIT)** au projet Sensibilisation à la cybersécurité et au projet Aide à la décision pour les cyberopérations défensives.

Objectif de la consultation

- Présenter les faits saillants de l'analyse du marché qui orientent notre approche de mise à profit des avantages économiques.

- Mettre en lumière les questions soumises à l'industrie dans la demande de renseignements.
  - La rétroaction fournie par l'industrie servira également à indiquer au gouvernement du Canada comment tirer le meilleur parti de ce contrat pour favoriser la croissance et l'innovation de l'industrie au Canada.

Politique des retombées industrielles et technologiques (RIT)

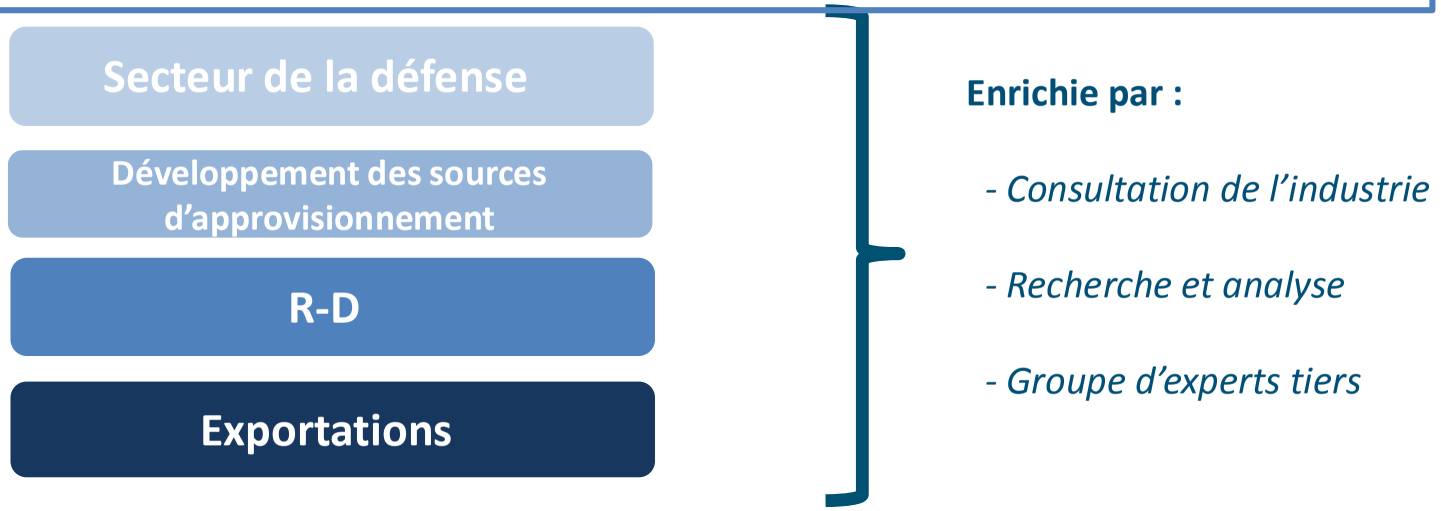
- **Les entreprises qui se voient attribuer des contrats d'approvisionnement en matière de défense sont tenues de mener des activités commerciales au Canada, dont la valeur équivaut à celle du contrat.**
- Quatre objectifs :

  - soutenir la viabilité à long terme et la croissance du secteur de la défense au Canada;
  - soutenir la croissance des entreprises et des fournisseurs au Canada, y compris les petites et moyennes entreprises de toutes les régions du pays;
  - améliorer l'innovation grâce à la R-D au Canada;
  - accroître le potentiel d'exportation des entreprises établies au Canada.

Proposition de valeur (PV)

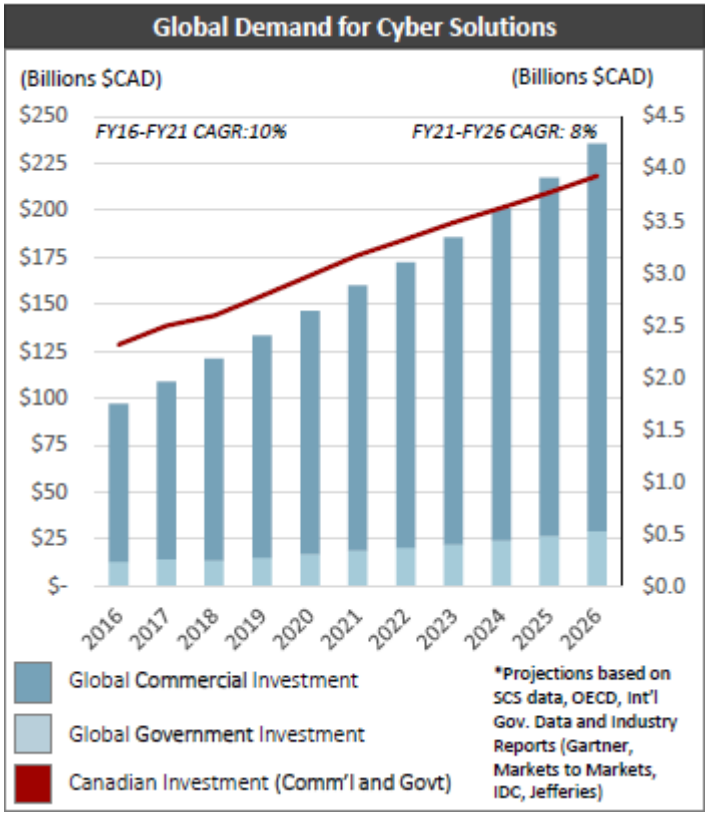
- **La proposition de valeur est ce que le soumissionnaire propose au Canada au moment de la soumission.**
- Le gouvernement du Canada développera un critère d'évaluation utilisé pour mesurer le niveau d'engagement d'un soumissionnaire à exécuter des travaux et à investir dans l'économie canadienne.
- Le critère d'évaluation de la PV :
  - elle sera enrichie par la consultation de l'industrie;
  - elle représentera un facteur pondéré dans la sélection du gagnant;
  - elle sera adaptée à chaque projet.

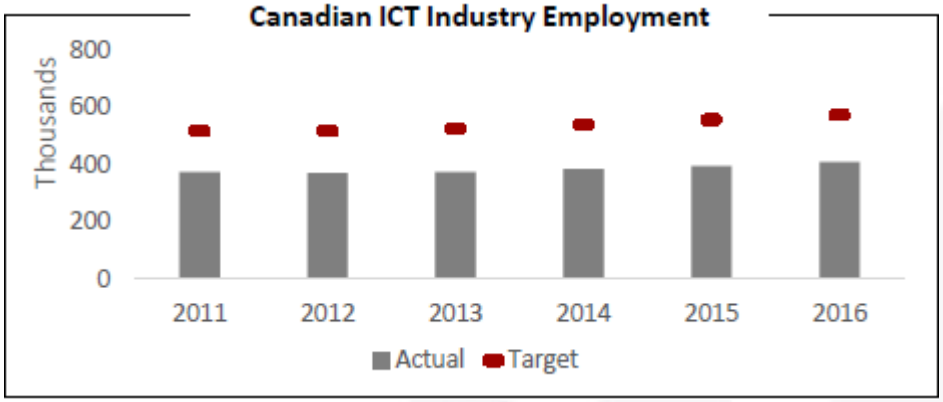
Une fois qu'un contrat est attribué, l'entrepreneur doit commencer à remplir ses obligations en matière de RIT et les engagements pris dans le cadre de la proposition de valeur.



Analyse du marché

- En raison de l'évolution rapide de la technologie de l'information et des menaces connexes, le cybermarché mondial passera d'environ 110 milliards de dollars en 2017 à plus de 163 milliards de dollars en 2021.
- On estime que le Canada compte 1 000 entreprises dans la vaste industrie des TIC, dont plus de 200 entreprises dans le marché de la cybersécurité.





Analyse du marché

- Grand espace concurrentiel comprenant des centaines d'entreprises dont la majorité sont des petites et moyennes entreprises.

- 98 % des entreprises canadiennes spécialisées dans le cyberespace ne s'intéressent pas au secteur de la défense et ciblent plutôt des clients dans le marché commercial qui est en croissance.

- La cyberinfrastructure existante était concentrée autour de grappes géographiques, y compris un milieu universitaire de calibre mondial, pouvant favoriser la cyberinnovation et servir de moteurs de croissance.

- Les domaines des points forts sur le plan technique au Canada comprennent :
  - l'intelligence artificielle;
  - l'informatique quantique;
  - la gestion de l'identité et de l'accès;
  - la prévention de la perte de données.

Key Observations for Leveraging Economic Benefits

- Le nombre élevé de **petites et moyennes entreprises** (PME) fait ressortir des possibilités de transfert de technologie, d'intégration de la chaîne d'approvisionnement et de partenariats avec de grandes entreprises afin de faire croître les PME et de mettre les technologies novatrices à l'échelle.

- Une demande accrue et une rentabilité à long terme dans le secteur commercial indiquent une propension d'investissement axé sur les **applications commerciales** de la cybertechnologie.

- Une pénurie dans le bassin de talents liés au cyberespace démontre l'importance d'investir dans le **développement des compétences et la formation** au sein de l'industrie et du milieu universitaire afin de renforcer la capacité nationale et de répondre aux besoins actuels et futurs en matière de main-d'œuvre.

- Il y a une solide base au Canada pour mener des activités avancées en R-D, de même que des possibilités de collaboration avec des établissements universitaires canadiens pour la **recherche et la commercialisation** de cybertechnologies.

- Le potentiel de l'**exportation** des cybertechnologies et des cyberservices est mitigé et les meilleures occasions sont axées sur les marchés traditionnels comme la collectivité des cinq et les alliés de l'OTAN.

Questions à l'intention de l'industrie

Veuillez consulter la DR – Annexe F – Politique des retombées industrielles et technologiques.

Secteur de la défense

Objectif : Promouvoir le développement économique et la viabilité à long terme des entreprises canadiennes chargées de la fabrication et de la prestation de produits et de services aux fins d'utilisation dans les applications de défense et de sécurité du gouvernement.

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

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

Développement des sources d'approvisionnement, y compris les PME

Objectif : Rendre l'industrie canadienne plus concurrentielle, indépendamment de l'entrepreneur ou du donateur éligible, en renforçant la productivité, le perfectionnement des compétences et la capacité de relever les défis du marché.

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

2. Quels types d'investissements le Canada devrait-il favoriser pour fournir aux entreprises canadiennes le plus de retombées possible dans le marché de la cybersécurité (secteur de la défense ou commercial)?
    a. Exemples :
        i. Création d'initiatives de formation et de développement de compétences afin d'attirer des travailleurs qualifiés et de les retenir (p. ex., codage et programmation, ingénierie des réseaux ainsi que développement et intégration de logiciels);
        ii. Investissements dans de nouveaux biens d'équipement et de nouvelles ressources;
        iii. Soutien en matière d'attestations de sécurité (p. ex., cote « Très secret » et ITAR) pour les entreprises canadiennes, surtout les petites et moyennes entreprises (PME);

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

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

Recherche et développement (R-D)

Objectif : Encourager la recherche scientifique qui explore le développement de nouveaux biens et services, de nouveaux intrants à la production et de nouvelles méthodes de production des biens et services, ou de nouvelles façons d'exploiter et de gérer des organismes.

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

2. Quels investissements de grande valeur en R-D réalisés au Canada, dans le secteur de la défense ou commercial, le Canada pourrait-il inciter les soumissionnaires à réaliser grâce à ces approvisionnements (p. ex., sécurité infonuagique, sécurité des appareils mobiles ou analyse de la sécurité)?
    a. Comment pourrait-on encourager les investissements dans les nouvelles technologies intersectorielles où le Canada offre des capacités (p. ex., l'informatique quantique, la réalité amplifiée/virtuelle ou l'intelligence artificielle/l'apprentissage machine)?

3. Pourrait-on créer des consortiums de recherche ou des centres d'excellence en partenariat avec des établissements d'études postsecondaires du Canada ou des établissements de recherche subventionnés par l'État ? Si c'est le cas, quels domaines de recherche votre entreprise pourrait-elle couvrir?
    a. Si non, quels autres partenariats en recherche ou en développement pourraient être créés pour soutenir le développement dans les domaines liés aux projets Sensibilisation à la cybersécurité et Aide à la décision pour les cyberopérations défensives?

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

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

Exportation

Objectif : Favoriser la capacité des entreprises canadiennes et des PME à exploiter avec succès les marchés d'exportation, ce qui accroît leur productivité et compétitivité dans les marchés mondiaux.

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

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

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

Questions supplémentaires

1. Compte tenu de l'importance de la cyberrésilience en tant que domaine de technologies émergentes, serait-il souhaitable que le Canada ait une pondération de la proposition de valeur, pour les projets de la SC et des CD-AD, supérieure à 10 % de l'évaluation globale de la soumission, en comparaison au prix et au mérite technique?

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

3. Est-ce que les projets Sensibilisation à la cybersécurité et Aide à la décision pour les cyberopérations défensives devraient inclure un volet de la proposition de valeur pour le développement des compétences?
   a. Si oui, quels types d'investissements et de partenariats dans le développement des compétences seraient les plus utiles pour le secteur canadien de la cybersécurité?

4. Dans quel secteurs d'activités, que ce soit dans le secteur de la défense ou dans le secteur commercial, existe-t-il des opportunités d'aider les entrepreneurs et entreprises autochtones, et les femmes entrepreneures ou les entreprises appartenant à des femmes au Canada?

Prochaine étapes

- Votre rétroaction servira à élaborer une stratégie visant à maximiser les avantages économiques découlant des contrats liés à la SC et aux CD-AD ainsi qu'à favoriser l'innovation dans le secteur canadien de la cybersécurité, y compris la croissance des entreprises canadiennes et la création d'emploi partout au pays.

- Pour obtenir de plus amples renseignements au sujet des retombées industrielles et technologiques et du Guide sur la proposition de valeur, rendez-vous à l'adresse suivante :

  http://www.canada.ca/rit

- Veuillez transmettre vos réponses écrites aux questions figurant à l'Annexe F de la DR à l'autorité contractante de SPAC.

National Defence Défense nationale

Aperçu des exigences opérationnelles

- Maj Martin Rivard, Directeur de projet, SC/CD-AD
- M. Raghu Balakrishnan, Chef de projet, SC/CD-AD

Canada

Ordre du jour

- Contexte
- Vision
- Vue opérationnelle
- Équipe de développement et de mentorat opérationnel
- Entités Cyber
- Fonctions et tâches de cyberdéfense
- Objectifs de performance
- Qualité des données et confiance
- Composants de l’Architecture Notionnelle
- Information requise

La politique

- Protection, Sécurité, Engagement : La politique de défense du Canada (juin 2017) (SSE #65 et SSE #87)
- Politique des retombées industrielles et technologiques (RIT)

Introduction : Une nouvelle politique de défense du Canada

INTÉRÊTS CANADIENS

Protection du Canada et des Canadiens □ Leadership dans le monde □ Stabilité mondiale et prévention des conflits, paix, prospérité et commerce □ Droits de la personne, inclusion et égalité entre les sexes

RAISONS MOTIVANT LE CHANGEMENT

Nouvelles sources de menaces

Instabilité et imprévisibilité croissantes, érosion de l'ordre mondial

Années de sous-financement et de gestion à court terme de l'effectif et des immobilisations à la Défense

Nouvelles possibilités

CHANGEMENTS PRINCIPAUX

Nouvelle politique et nouveaux investissements

Changements structuraux

COUP D'OEIL SUR
PROTECTION. SÉCURITÉ. ENGAGEMENT.

PROTECTION AU CANADA

- Amélioration de la surveillance et du contrôle aériens et maritimes, notamment dans l'Arctique
- Intervention simultanée en cas de multiples urgences nationales
- Soutien à la lutte contre le terrorisme
- Soutien à la recherche et sauvetage
- Prendre soin de nos gens

SÉCURITÉ EN AMÉRIQUE DU NORD

- Modernisation du NORAD
- Augmentation du contrôle et de la connaissance des domaines aérospatiaux et maritimes
- Recherche de pointe dans le domaine de la défense

ENGAGEMENT DANS LE MONDE

Des FAC prêtes à mener simultanément :

- 2 déploiements majeurs prolongés
- 1 déploiement majeur à durée limitée (6 à 9 mois)
- 2 déploiements mineurs prolongés et 2 déploiements mineurs à durée limitée
- 1 mission de l'Équipe d'intervention en cas de catastrophe (EICC)
- 1 opération d'évacuation de non-combattants

NOUVELLES INITIATIVES

Nos gens d'abord

- Nouvelle stratégie **Santé et bien-être globaux**
- Réinvention de la **transition des malades/blessés** au service actif ou à la vie civile
- **Allègements fiscaux** pour les opérations de déploiement
- Prendre soin des **familles**
- **Intégration de l'ACS+** et atteinte des cibles quant à **l'égalité entre les sexes** et la **diversité**
- **Ajout de 3 500 membres de la Force régulière** pour les priorités principales
- **Ajout de 1 500 membres de la Force de réserve :** Capacité à temps plein; service à temps partiel
- **Ajout de 1 150 civils** pour appuyer les opérations

Investissements dans la force future

- **Investissement** supplémentaire de 62 G$ en immobilisations, dont les dépenses passent à 104 G$
- Rétablissement des **capacités principales** : **88** chasseurs perfectionnés, **15** navires de combat de surface, **2** navires de soutien interarmées, **6** navires de patrouille extracôtiers et de l'Arctique
- Augmentation des capacités dans les domaines émergents – **cyberespace**, **espace** et **véhicules télépilotés** – pour maintenir l'efficacité et l'interopérabilité avec les alliés
- Augmentation des capacités, notamment dans les domaines du **renseignement**, des **communications par satellite**, de la **surveillance** et des **véhicules logistiques**

Modernisation des activités de défense

- **Programme d'innovation transformateur** comprenant des groupes de recherche en défense liés à l'approvisionnement
- Processus d'**approvisionnement en matière de défense** plus responsable, transparent et rationalisé
- **Réduction de l'empreinte carbone** en favorisant les infrastructures écologiques et l'efficacité énergétique
- Modernisation de la **gestion des infrastructures** en élargissant le partenariat avec le secteur privé

Contexte

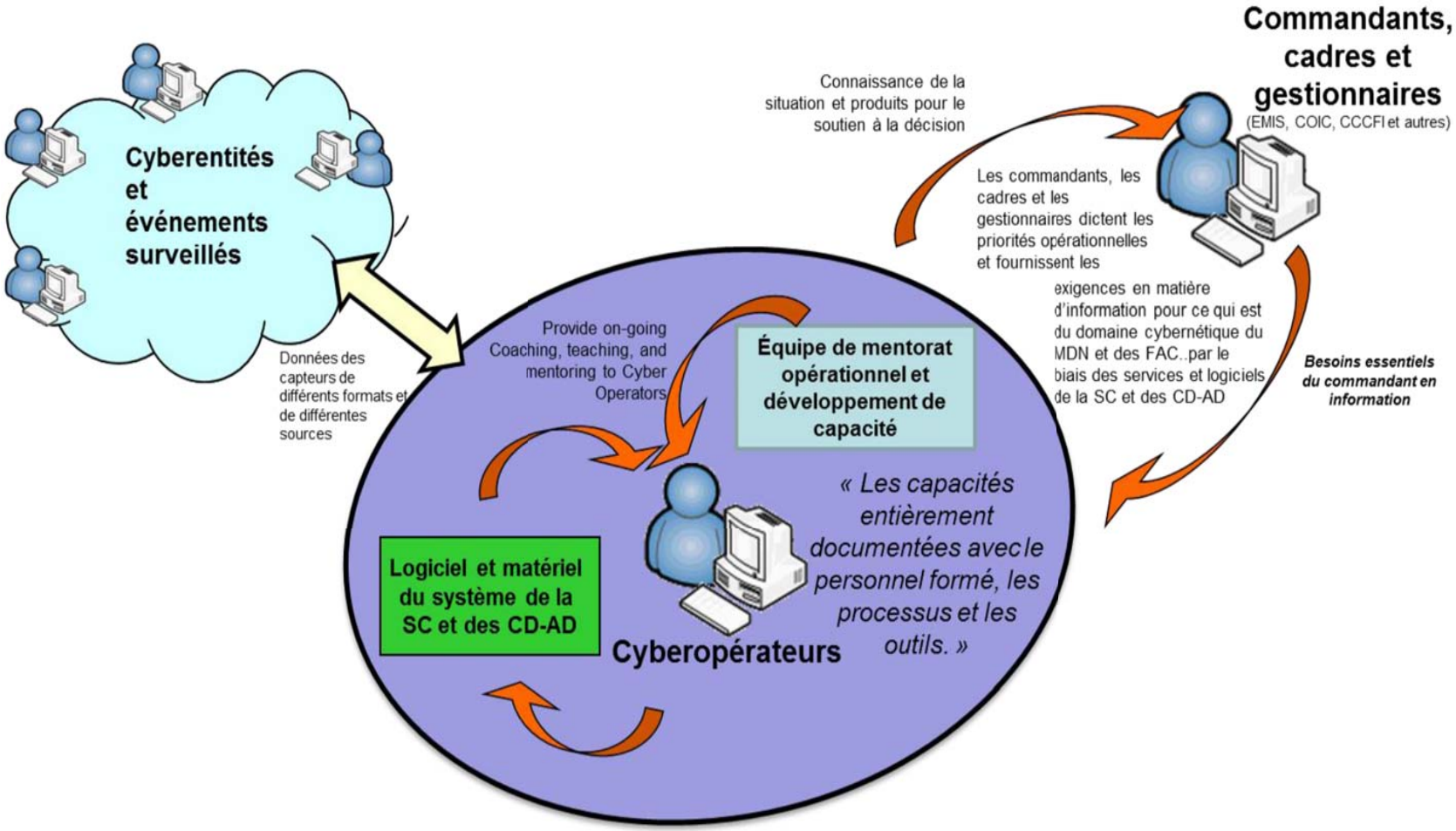
- Le **projet de SC** transformera la façon dont le MDN et les FAC gèrent la confidentialité, l'intégrité et la disponibilité du cyberespace de plus en plus complexe du MDN et des FAC. Cela sera accompli en se concentrant sur l'identification et la sécurisation de son cyberespace, en fournissant une connaissance de la situation de bout en bout qui permettra aux commandants de prendre des décisions éclairées concernant la posture de sécurité de leur cyberespace.

- Le **projet CD-DA** améliorera la capacité du MDN et des FAC à mener des opérations cyber défensives. Ceci sera accompli en fournissant une capacité de réponse contre les menaces avancées, et en améliorant la prise de décision, rendant le processus plus agile, réactif et efficace afin de maintenir la liberté de manœuvre des commandants dans le cyberespace

Vision

La vision du projet SC et CD-AD est de fournir aux FAC une capacité durable à la fine pointe de la technologie pour mener des opérations de cybersécurité. .

Vue opérationnelle



La tâche des cyber-opérateurs

- Dans le contexte des projets CSA et DCO-DS, la tâche des cyber-opérateurs est de:
  - «Sécuriser le cyberdomaine du MDN et des FAC pour soutenir la défense du Canada»

- Pour que cette tâche soit couronnée de succès, les cyber-opérateurs ont besoin d'outils et de procédures pour:
  - détecter, reconnaître et identifier les cyber-entités hostiles ou non autorisées dans le cyber-domaine MDN / FAC, et
  - Fournir aux commandants, aux cadres supérieurs et aux gestionnaires les renseignements opportuns pour prendre des décisions éclairées.

Cyberentités

- « toute chose distincte ou acteur distinct qui existe dans l'infrastructure cybernétique [cyberespace] »

  - **Cyberentités non humaines.** Ce sont des éléments du système participant (physiques ou virtuels) tels que les postes de travail, les routeurs, les commutateurs, les processus, les fichiers, les serveurs et la mémoire. Le tableau de l'appendice 2 de la présente annexe énumère les attributs clés qui doivent (le cas échéant) être collectés pour chaque cyberentité non humaine.
  - **Cyberentités humaines.** Ce sont des personnes réelles et leurs personnages opérant dans le cyberespace. Le tableau de l'appendice 3 de la présente annexe énumère les attributs clés qui doivent (le cas échéant) être collectés pour chaque cyberentité humaine.

Mentorat opérationnel et développement de capacité (MODC)

- Les services professionnels, sous forme d'équipes de MODC, seront regroupés avec la capacité fournie pendant la mise en œuvre et tout au long de son cycle de vie.

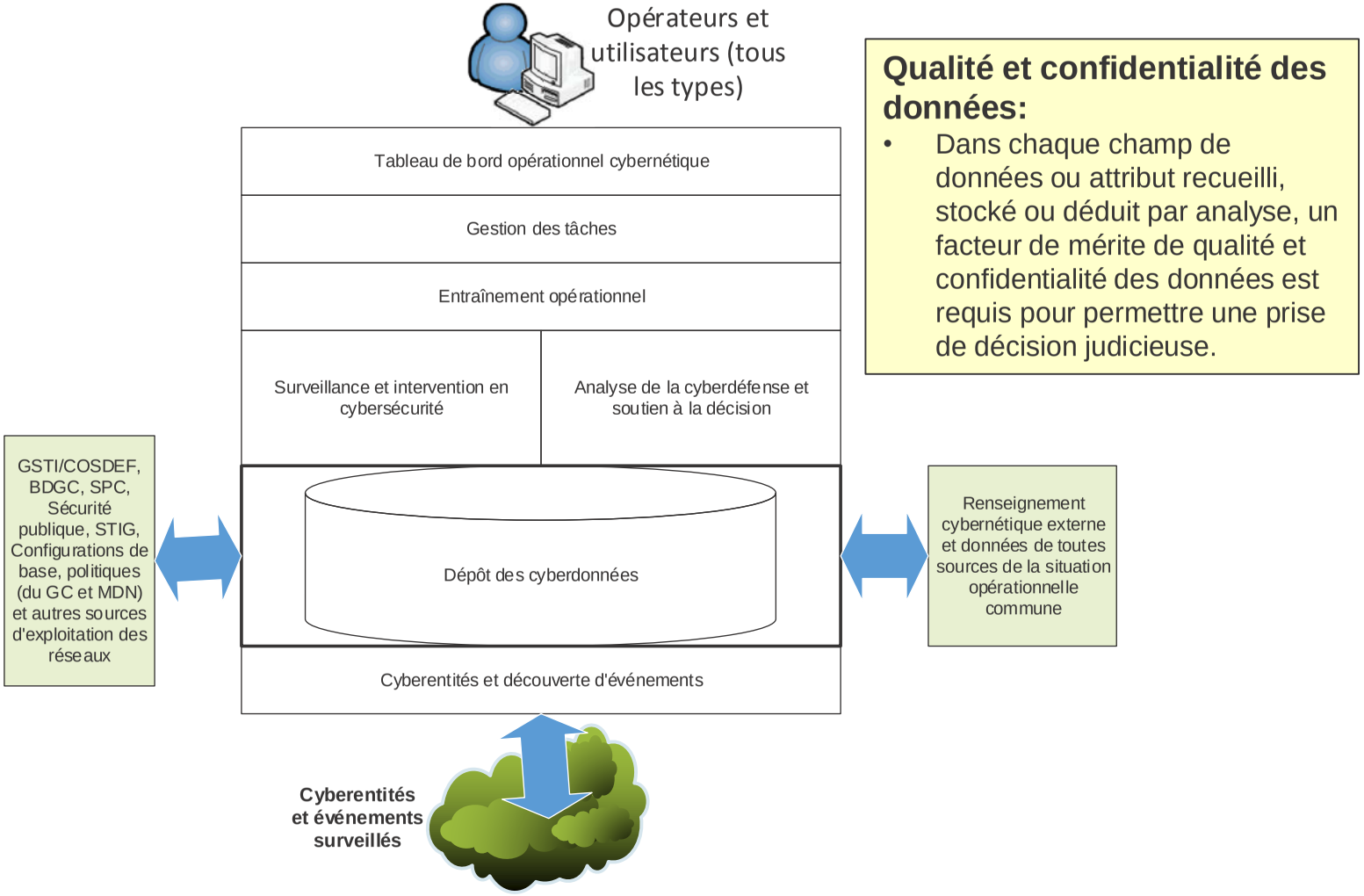
- Le rôle des équipes de MODC est d'entraîner, de former et de guider les cyberopérateurs (de tous les grades):
  - soutenir la transformation opérationnelle des capacités de cybersécurité et des CD des FAC afin qu'elles deviennent des capacités d'opérations de sécurité de niveau 5 du NIST;
  - soutenir les opérations de cybersécurité et les CD;
  - guider les cyberpérateurs à tous les niveaux pour améliorer leurs compétences et améliorer les cyberopérations des FAC afin d'assurer le maintien des compétences.

Objectifs de performance de la capacité

… détecter, reconnaître et identifier les cyber-entités hostiles ou autrement non autorisées au sein du cyber domaine du MDN et des FAC, et fournir aux commandants, aux cadres supérieurs et aux gestionnaires les renseignements opportuns pour prendre des décisions éclairées..

Response Time	Activity
En quelques secondes	**But: DÉTECTION.** Détecter qu'une Entité Cyber est devenue active (connectée) et initier des réponses automatiques appropriées à la situation. Initiez la collecte et le contrôle des données.
En quelques minutes	**But: RECONNAISSANCE** et **IDENTIFICATION.** Déterminer la nature d'une entité virtuelle (ami ou ennemi), ses attributs clés et initier des réponses automatisées appropriées à la situation. Continuer la collecte et le contrôle des données.
En une heure	**But**: **IDENTIFICATION** avec classification et attribution complètes pour initier des actions plus complètes.
En une journée	**But**: **Mise à jour de l'analyse des menaces et des risques** et de la planification défensive, appuyée par la collecte de données judiciaires et de renseignements en cours.
En une semaine	**But**: Mettre en œuvre de nouvelles techniques de défense opérationnelles avec de nouvelles tactiques, techniques et procédures basées sur les leçons apprises.
En un mois	**But**: Faire évoluer la posture de sécurité globale du domaine cyber du MDN / des FAC vers une capacité défensive améliorée.

Vue architecturale des composants notionnels



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.

Information Requested

- Section 1: Sommaire
- Section 2: Profil de l’entreprise
- Section 3: Concept de solution proposé. Les répondants sont priés de fournir ce qui suit:
  - Aperçu du plan de solution
  - Plan détaillé de haut niveau et séquence d'événements
  - Coûts estimés pour chaque livrable (utiliser l'approche de la vue d'architecture des composants notionnels si possible)
    - une estimation des coûts indicatifs, accompagnée d'une description par unité, pour tout produit livrable défini à l'annexe B que le répondant a l'intention de fournir.
    - Coût = prix / unité x nombre d'unités
- Section 4: Commentaires et conseils généraux

Ceci est essentiel pour aider le projet à développer un budget de projet pour le processus d'approbation.

Informations clés sur les prix requises

- Gestion de projet, ingénierie d'intégration et conception de systèmes et documentation à l'appui
- Tout le matériel, les logiciels, l'installation, la configuration du système et les tests d'acceptation
- Services de transformation commerciale
- Système de soutien en service et services d'ingénierie professionnelle
- Formation initiale-cadre
- Il est essentiel que les modèles de tarification soient évolutifs en fonction de:
  - Nombre d'utilisateurs sur le réseau?
  - Nombre de points de présence ou de sites?
  - Nombre de nœuds clés ou de serveurs?
  - Nombre d'événements par seconde par périphérique, actif informatique, entité Cyber, etc.
  - Ou une combinaison de ci-dessus

QUESTIONS

REMARQUES DE CLÔTURE

JE VOUS REMERCIE!