



**RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:**

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

**LETTER OF INTEREST
LETTRE D'INTÉRÊT**

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 sécurité et des opérations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Title - Sujet LI - GIJA	
Solicitation No. - N° de l'invitation W8474-19AM01/A	Date 2018-11-06
Client Reference No. - N° de référence du client W8474-19AM01	GETS Ref. No. - N° de réf. de SEAG PW-\$\$QE-063-27048
File No. - N° de dossier 063qe.W8474-19AM01	CCC No./N° CCC - FMS No./N° VME
Solicitation Closes - L'invitation prend fin at - à 02:00 PM on - le 2018-12-17	
Time Zone Fuseau horaire Eastern Standard Time EST	
F.O.B. - F.A.B. Plant-Usine: <input type="checkbox"/> Destination: <input type="checkbox"/> Other-Autre: <input type="checkbox"/>	
Address Enquiries to: - Adresser toutes questions à: Norris, Chantale	Buyer Id - Id de l'acheteur 063qe
Telephone No. - N° de téléphone (819) 420-1758 ()	FAX No. - N° de FAX (819) 956-6907
Destination - of Goods, Services, and Construction: Destination - des biens, services et construction: Specified Herein Précisé dans les présentes	

Instructions: See Herein

Instructions: Voir aux présentes

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	

Le projet de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)

Lettre d'intérêt

TABLE DES MATIÈRES

PARTIE I : PROCESSUS RELATIF À LA LETTRE D'INTÉRÊT	1
1. INTRODUCTION.....	1
2. CONSIGNES À SUIVRE POUR RÉPONDRE À LA PRÉSENTE LETTRE D'INTÉRÊT	2
PARTIE II : SOLUTION DE GIJIA.....	4
1. CONTEXTE DU PROJET DE GIJIA	4
2. OBJECTIF DE LA PRÉSENTE LI	4
3. EXIGENCES EN MATIÈRE DE SÉCURITÉ	4
4. EXCEPTION AU TITRE DE LA SÉCURITÉ NATIONALE	5
5. APPLICATION DE LA POLITIQUE DES RETOMBÉES INDUSTRIELLES ET TECHNOLOGIQUES (RIT)	5
6. LANGUES OFFICIELLES	6
7. APPROCHE EN MATIÈRE D'ENGAGEMENT	6
PARTIE III : QUESTIONS À L'INDUSTRIE	11
1. QUESTIONS À L'INDUSTRIE.....	11

ANNEXE A : CAPACITÉ ET PROJET DE GESTION DE L'IDENTITÉ, DES JUSTIFICATIFS D'IDENTITÉ ET DE L'ACCÈS (GIJIA)

OBJET ET CONTENU DE LA PRÉSENTE LETTRE D'INTÉRÊT

La présente lettre d'intérêt (LI) porte sur le projet de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) pour le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC). L'objet de la présente LI est d'orienter et de préparer l'industrie en vue d'éventuelles possibilités d'approvisionnement concernant le projet de GIJIA et de recueillir des commentaires et la contribution en ce qui a trait à la portée, aux exigences, au calendrier et aux risques du projet. Le contenu général de la présente LI comprend :

PARTIE I : Processus relatif à la lettre d'intérêt – Renseignements sur le processus de la LI et la procédure que doit suivre l'industrie pour répondre à la présente LI

PARTIE II : Solution de GIJIA

PARTIE III : Questions à l'intention de l'industrie – Questions qui visent à obtenir la rétroaction de l'industrie et qui permettront au MDN et aux FAC de définir leurs besoins et leur analyse de rentabilisation

ANNEXE A : Contexte du projet de GIJIA

PARTIE I : PROCESSUS RELATIF À LA LETTRE D'INTÉRÊT

1. INTRODUCTION

Le projet de GIJIA en est à la phase précoce d'analyse des options, ce qui signifie que l'analyse de rentabilisation et la justification du projet sont encore en cours d'élaboration. Ainsi, aucune décision sur les concepts, les technologies ou les solutions n'a été prise. L'objectif de la phase d'analyse des options est de s'assurer que les cadres supérieurs du Ministère peuvent prendre une décision éclairée sur la meilleure façon de définir le projet (c.-à-d. mener la phase de définition) et, si cela est jugé approprié, mettre en œuvre le projet afin de réaliser la capacité requise.

L'intention est de mobiliser et de consulter activement l'industrie pendant les phases d'analyse des options et de définition afin d'assurer la réussite du projet. La rétroaction de l'industrie aidera l'équipe de projet du MDN et des FAC à définir ce qui suit :

- a. L'énoncé des besoins (EB) d'une manière compréhensible pour l'industrie et pertinente dans le contexte opérationnel du MDN et des FAC, et ainsi contribuer à bien décrire les besoins opérationnels;
- b. L'« art du possible » concernant les capacités en matière de GIJIA, l'évolution future au sein de l'industrie et la manière dont les grandes entreprises changent pour répondre à leurs besoins informatiques en évolution, ce qui permet de bien définir l'EB, le budget et le calendrier requis pour atteindre les objectifs du projet (du point de vue technologique et industriel / de l'approvisionnement);
- c. Les répercussions sur les personnes, les processus et la technologie des diverses solutions proposées ainsi que les changements organisationnels qui seront nécessaires à l'appui de chaque solution conceptuelle;
- d. La stratégie d'approvisionnement la plus appropriée qui soit acceptable pour l'industrie pour fournir le bon équipement au MDN et aux FAC en temps opportun, obtenir le maximum de l'argent des contribuables, mettre à profit les achats pour créer des emplois et de la croissance, et simplifier les processus d'approvisionnement.

Le MDN et les FAC ne communiqueront pas avec les fournisseurs à la suite de cette LI. L'autorité contractante présentée à la section 2.7 pourrait communiquer avec l'industrie pour obtenir plus de renseignements à propos des réponses. Toute activité future de mobilisation ou d'approvisionnement de l'industrie sera diffusée publiquement.

1.1 Nature de la présente lettre d'intérêt

Ceci n'est pas une demande de soumissions. La présente LI ne donnera lieu ni à l'attribution d'un contrat ni à la création d'une quelconque liste de fournisseurs. Les fournisseurs éventuels de biens ou de services décrits dans la présente LI ne doivent pas réserver de stocks ou d'installations ni affecter des ressources en fonction des renseignements présentés dans celle-ci. Par conséquent, qu'un fournisseur éventuel réponde ou non à cette LI ne l'empêchera pas de participer à un processus d'approvisionnement ultérieur.

De plus, la présente LI ne mènera pas nécessairement à l'acquisition des biens et services qui y sont décrits. La présente LI vise simplement à obtenir des commentaires de l'industrie sur les éléments qui y sont présentés.

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

2.1 Nature et présentation des réponses demandées

On rappelle aux répondants que ce document est une LI et non une demande de propositions (DP). Ainsi, les répondants sont invités à livrer leurs commentaires, leurs préoccupations et leurs recommandations quant à la façon dont les exigences ou les objectifs décrits dans cette LI pourraient être satisfaits. Ils devraient prendre soin d'expliquer toute hypothèse énoncée dans leurs réponses.

Les réponses ne seront pas utilisées à des fins d'évaluation compétitive ou comparative, et par conséquent, elles n'ont pas besoin d'être données dans un format aussi rigide que le seraient les réponses à une DP. Toutefois, pour faciliter l'utilisation et pour maximiser la valeur des réponses, le Canada demande que les répondants suivent le format présenté à la section.

2.2 Coûts relatifs aux réponses

Le Canada ne remboursera aucuns frais engagés par les organismes pour répondre à la présente LI.

2.3 Traitement des réponses

Utilisation des réponses : Les réponses ne feront pas l'objet d'une évaluation formelle; le gouvernement du Canada pourra utiliser les réponses reçues afin d'élaborer ou de modifier sa stratégie d'approvisionnement. Le Canada procédera à l'examen de toutes les réponses reçues. Le Canada peut, à sa discrétion, examiner des réponses reçues après la date de clôture de la LI.

Équipe d'examen : Une équipe d'examen composée de représentants du MDN et de Services publics et Approvisionnement Canada (SPAC) examinera les réponses. Le Canada se réserve le droit d'embaucher des experts-conseils indépendants ou d'utiliser des ressources du gouvernement du Canada, pour l'examen des réponses, s'il le juge nécessaire. Chaque réponse ne sera pas nécessairement examinée par tous les membres de l'équipe d'examen.

Confidentialité : Les répondants devraient indiquer les parties de leur réponse qu'ils considèrent comme étant exclusives ou confidentielles. Le Canada traitera ces réponses, conformément aux exigences de la *Loi sur l'accès à l'information*.

2.4. Communication avec l'industrie

L'autorité contractante peut communiquer avec l'industrie pour obtenir plus de renseignements à propos d'une réponse.

2.5 Contenu de la lettre d'intérêt

Les renseignements contenus dans le présent document évoluent constamment. C'est pourquoi les répondants ne doivent pas perdre de vue que de nouvelles exigences pourraient être ajoutées à toute demande de soumissions que publiera éventuellement le Canada. Les répondants ne doivent pas non plus supposer qu'aucune des exigences ne sera supprimée ou révisée. Les répondants sont donc invités à faire part de leurs commentaires sur tout aspect des exigences. La présente LI contient également des questions précises adressées à l'industrie.

2.6 Format de présentation des réponses

Page couverture : si la réponse comprend plusieurs volumes, le répondant doit indiquer, sur la page couverture de chacun des volumes, le titre de la réponse, le numéro de la LI, le numéro du volume ainsi que la dénomination sociale complète du répondant.

Page titre : La première page qui suit la page de couverture doit représenter la page titre. Celle-ci doit

comporter les éléments suivants :

- 2.6.1 Le titre de la réponse et le numéro du volume;
- 2.6.2 Le nom et l'adresse du répondant;
- 2.6.3 Le nom, l'adresse et le numéro de téléphone du représentant du répondant;
- 2.6.4 La date;
- 2.6.5 Le numéro de la LI.

Nombre de copies : Le Canada demande que les répondants présentent leur réponse en format PDF [en version 2003 ou plus récente] non protégé (c.-à-d. sans mot de passe). Si la taille du document est inférieure à six mégaoctets (Mo), le Canada demande aux répondants de l'envoyer par courriel à TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca. Si la taille du document PDF est égale ou supérieure à 6 Mo, le Canada demande aux répondants d'en enregistrer une copie sur deux clés USB et de les envoyer par la poste à l'agent des contrats dont les coordonnées figurent à la section 2.7.

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

2.7 Demandes de renseignements

Toutes les demandes de renseignements et autres communications relatives à la présente LI doivent être présentées uniquement directement à l'autorité contractante de SPAC. Comme il ne s'agit pas d'une demande de soumissions, le Canada ne répondra pas nécessairement par écrit et ne donnera pas forcément de réponses à tous les répondants; toutefois, les répondants qui ont des questions concernant la présente LI peuvent les transmettre à :

Autorité contractante : Chantale Norris
Services publics et Approvisionnement Canada
Place du Portage III, bureau 8C2
11, rue Laurier Gatineau (Québec) K1A 0S5
819-420-1758
Adresse courriel : TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Veillez inscrire « LI SUR LE PROJET DE GIJA » sur la ligne objet pour éviter un retard de la réponse.

Le courriel électronique est la méthode préféré de communication.

2.8 Présentation des réponses

Date et lieu de présentation des réponses : Les organisations souhaitant fournir une réponse doivent la remettre à l'autorité contractante indiquée à la page 1 de la présente LI, au plus tard à la date et à l'heure de clôture indiquées à la page 1 de la présente demande de soumissions.

La date de clôture de la LI n'est pas la date limite pour présenter des commentaires ou des contributions. Les commentaires et les contributions seront acceptés jusqu'à ce qu'un suivi concernant la demande de soumissions soit publié.

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

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

PARTIE II : SOLUTION DE GIJIA

1. CONTEXTE DU PROJET DE GIJIA

Les contrôles de l'accès au sein du ministère de la Défense nationale (MDN), et entre le MDN et ses partenaires au Canada et à l'étranger, sont complexes et sujets à des risques émanant de menaces internes et externes.

La multiplication des renseignements sur l'identité et sur les justificatifs d'identité à l'échelle du MDN devrait être rationalisée afin de réduire la perte, l'endommagement ou la compromission de renseignements.

La rationalisation des processus liés à la GIJIA est nécessaire afin de rendre les utilisateurs plus productifs, sécuriser davantage les ressources, rendre les décisions plus transparentes et faciliter la vérification des mesures. Plus précisément, la modernisation de la GIJIA permettra :

- de fournir aux employés une plus grande visibilité pour ce qui est des renseignements personnels liés à leur identité, et la possibilité de mettre à jour leur profil;
- d'atténuer les cybermenaces;
- d'appuyer les enquêtes judiciaires sur les infractions liées à l'accès.

En bref, les Forces armées canadiennes (FAC) du MDN souhaitent moderniser et améliorer l'interopérabilité, la rapidité, l'exactitude et la confidentialité de ses données sur l'identité, des justificatifs d'identité et des contrôles de l'accès aux installations matérielles, aux renseignements et aux systèmes d'information. Cela comprend l'amélioration de l'interopérabilité entre les FAC du MDN et leurs partenaires d'autres ministères et organismes gouvernementaux, d'alliés et du secteur privé.

2. OBJECTIF DE LA PRÉSENTE LI

La présente LI est publiée aux fins suivantes :

- 2.1. consulter l'industrie pour mieux comprendre les possibilités offertes et émergentes en matière d'infrastructure commerciale de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) et de solutions de service;
- 2.2. Obtenir des renseignements pour aider le MDN et les FAC à établir leurs besoins et aider au processus interne de planification et d'approbation pouvant mener à une demande de soumissions;
- 2.3. Obtenir des renseignements pour aider le MDN et les FAC à regrouper éventuellement certains des produits livrables, afin qu'un fournisseur ou une équipe de fournisseurs puisse offrir une solution intégrée pour un sous-ensemble cohérent de produits livrables.

La présente LI ne signifie pas que le Canada a pris une décision définitive quant aux possibilités d'approvisionnement. Le MDN et les FAC peuvent décider de ne choisir aucune des solutions ou aucun équipement indiqués dans les réponses. En aucune circonstance, le Canada ne sera tenu responsable à l'égard d'un fournisseur ayant préparé une réponse à la présente LI.

3. EXIGENCES EN MATIÈRE DE SÉCURITÉ

Aucune exigence relative à la sécurité n'est liée à la présente LI.

Pour toute mesure d'approvisionnement prise à l'appui de la présente solution de GIJIA, les fournisseurs pourraient être tenus de disposer d'une cote de sécurité de niveau II (Secret) émise par leur organisme de sécurité nationale respectif. Certains fournisseurs pourraient également devoir satisfaire aux

exigences du gouvernement du Canada relatives à la fourniture de produits et de services comportant des restrictions liées à la classification « Réservé aux Canadiens ».

3.1 VIE PRIVÉE

Le Canada a l'obligation de veiller au respect des lois, des règlements et des politiques du pays qui ont trait à la protection des renseignements personnels. S'il faut traiter des renseignements personnels dans le cadre d'un contrat subséquent, le Canada pourrait demander aux fournisseurs de se conformer aux dispositions sur la protection des renseignements personnels prévues dans la [Loi sur la protection des renseignements personnels](#) (L.R.C., 1985, ch. P-21), la [Loi sur la protection des renseignements personnels et les documents électroniques](#) (2000, ch. 5) et dans d'autres instruments de politiques fédéraux concernant la confidentialité.

4. EXCEPTION AU TITRE DE LA SÉCURITÉ NATIONALE

Afin de protéger les intérêts de sécurité nationale, le Canada invoquera son droit en vertu des accords commerciaux nationaux et internationaux d'utiliser une exception au titre de la sécurité nationale (ESN) dans le cadre du présent processus d'approvisionnement. L'ESN permet au Canada de soustraire un processus d'approvisionnement de certaines ou de l'ensemble des obligations d'un accord commercial visé lorsqu'il le juge nécessaire afin de protéger ses intérêts en matière de sécurité nationale ou des intérêts connexes indiqués dans le texte des ESN.

5. POLITIQUE DES RETOMBÉES INDUSTRIELLES ET TECHNOLOGIQUES (RIT)

5.1 Application de la politique des retombées industrielles et technologiques (RIT)

La Politique des retombées industrielles et technologiques (RIT), y compris la proposition de valeur, pourrait s'appliquer au projet de gestion de l'identité et des droits d'accès (GIDA). L'engagement pris au moyen de la lettre d'intérêt aidera à déterminer l'applicabilité de la Politique des RIT et la façon dont le Canada peut recourir à ce marché pour en tirer un avantage économique.

5.2 La Politique des RIT, y compris la proposition de valeur

La Politique des RIT est un outil puissant qui sert à attirer des investissements. Les entreprises qui concluent des marchés d'approvisionnement en matière de défense sont tenues de mener des activités commerciales au Canada dont la valeur équivaut à celle du marché. La Politique des RIT encourage les entreprises à s'établir au Canada ou à y accroître leur présence, à renforcer leurs chaînes d'approvisionnement au pays et à développer des capacités industrielles canadiennes.

La Politique des RIT vise à soutenir la viabilité à long terme et la croissance du secteur de la défense du Canada, y compris les petites et moyennes entreprises de partout au pays, à stimuler l'innovation au Canada au moyen de la R-D, à soutenir le perfectionnement des compétences et la formation ainsi qu'à accroître le potentiel d'exportation des entreprises établies au Canada. 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.

Pour de plus amples renseignements sur la Politique des RIT, rendez-vous à l'adresse www.canada.ca/rit.

5.2.1 Capacités industrielles clés:

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 du secteur de la défense à investir dans les [Capacités industrielles clés](#) (CIC). Les CIC sont en harmonie avec la politique de défense du Canada, [Protection, Sécurité, Engagement](#), et le [Plan pour l'innovation et les compétences](#) en soutenant le développement

des compétences et en favorisant l'innovation dans le secteur de la défense du Canada. Les CIC sont liées à des domaines de technologies émergentes qui présentent un potentiel de croissance rapide et des débouchés importants, à des capacités établies par rapport auxquelles le Canada est concurrentiel à l'échelle mondiale et à des domaines où la capacité nationale est essentielle à la sécurité du pays.

Le gouvernement a identifié cet approvisionnement nécessitant des capacités dans le domaine de la cyberrésilience. En tant que technologie émergente, la cyberrésilience a été identifiée comme un domaine présentant un potentiel de croissance rapide et d'innovation. Pour cette raison, le Canada désire créer de nouveaux débouchés dans ce domaine de technologie émergente et pour ce faire, encouragera les partenariats et les investissements auprès du secteur et d'établissements postsecondaires appuyant le perfectionnement des connaissances, de même que la recherche et le développement.

Voici la définition de la CIC concernée par ce projet :

Cyberrésilience

La cyberrésilience couvre tous les aspects des secteurs de la sécurité nationale, civile et commerciale, et rectifie les vulnérabilités créées par l'expansion de la technologie de l'information et de l'économie du savoir. La cyberrésilience comporte des activités de conception, d'intégration et de mise en œuvre de solutions technologiques qui protègent l'information et les réseaux de communication. Ces technologies, parmi d'autres, doivent être axées sur le développement efficace des cybercapacités suivantes :

Sécurité de l'information

La protection des données et des renseignements électroniques et numériques contre l'accès et toute intrusion, l'utilisation, la divulgation, la perturbation, la modification, la consultation, l'inspection, l'enregistrement ou la destruction non autorisé.

Sécurité informatique

La sécurisation du contenu et la gestion des menaces (point terminal, messagerie, réseaux, Web, nuage), sécurité, gestion des vulnérabilités et des risques, gestion de l'identité et de l'accès, et autres produits (p. ex. des trousseaux de chiffrement et de gestion des jetons, et des essais de vérification de produits de sécurité), ainsi que des services d'éducation, de formation et de connaissance de la situation.

Sécurité des technologies opérationnelles

La surveillance, mesure et protection des systèmes d'automatisation et de contrôle des processus industriels et connexes. La cyberrésilience peut comprendre la création d'outils et l'intégration de systèmes et de processus qui renforcent la sécurité des systèmes tactiques ou des grands réseaux, le chiffrement, la cyber-expertise et les interventions en cas d'incident, entre autres. Les capacités établies dans ce domaine pourraient s'appuyer de plus en plus sur l'IA à titre de technologie habilitante. Ainsi, des réseaux feraient usage de leurs défenses de façon autonome et dynamique contre les intrusions et se répareraient eux-mêmes après une perturbation.

6. LANGUES OFFICIELLES

Tout marché futur visant une solution de GIJIA pourrait exiger que l'entrepreneur fournisse tous les documents ainsi que le soutien technique et le soutien aux clients dans les deux langues officielles.

7. APPROCHE EN MATIÈRE D'ENGAGEMENT

7.1 Mobilisation de l'industrie

Le processus de mobilisation de l'industrie commence avec la présente LI et prendra fin au moment

où une demande de renseignements officielle, une DP ou un autre processus concurrentiel sera envoyé aux fournisseurs.

La présente LI est publiée sur <https://achatsetventes.gc.ca/> afin de permettre à l'industrie d'échanger des renseignements avec SPAC et le MDN sur la situation actuelle du marché, les technologies disponibles et les capacités des fournisseurs.

Étant donné que le MDN et les FAC en sont à la phase précoce de l'analyse des options du présent processus d'approvisionnement, l'approche de mobilisation de l'industrie au-delà de la présente phase est toujours en cours d'élaboration.

PARTIE III : QUESTIONS À L'INDUSTRIE

1. QUESTIONS À L'INDUSTRIE

1.1. Domaines d'intérêt

- 1.1.1 Quelles solutions fournies par votre entreprise pourraient aider le ministère de la Défense nationale (MDN) à réaliser les capacités présentées dans l'architecture conceptuelle de la Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) décrite à l'annexe A?
- 1.1.2 Quel rôle votre entreprise pourrait-elle possiblement chercher à remplir? (p. ex. intégrateur de systèmes principal, intégrateur de sous-systèmes ou fournisseur de produits)

5.1 Gouvernance

Que pourriez-vous offrir au MDN dans le domaine de l'établissement ou de l'amélioration de la gouvernance, de la politique, des normes, des lignes directrices et des processus en matière de GIJIA? Quelle est l'expérience de votre entreprise dans ces domaines?

5.2 Expérience du soutien d'exigences militaires

- 1.3.1 Votre entreprise a-t-elle déjà réalisé des projets de soutien d'exigences militaire?
- 1.3.2 Quelle est l'expérience de votre entreprise dans la réalisation ou le soutien de capacités de réseau dans un contexte militaire?
- 1.3.3 Quelle est l'expérience de votre entreprise dans le soutien d'accès aux installations dans un contexte militaire?
- 1.3.4 Votre entreprise a-t-elle de l'expérience en matière de processus d'accréditation et d'autorisation de sécurité pour le MDN?

5.3 Expérience dans l'exécution de solutions de GIJIA

- 1.4.1 Quelle est l'expérience de votre entreprise dans l'exécution de solutions de GIJIA? Pourriez-vous résumer les solutions fournies?
- 1.4.2 Quelle est l'expérience de votre entreprise dans le traitement de « données douteuses » et pourriez-vous résumer l'approche recommandée pour le nettoyage des données? [Les données douteuses, ou indésirables, sont des données inexactes, incomplètes ou incohérentes contenues dans un système informatique ou une base de données. Les données douteuses peuvent contenir des fautes d'orthographe ou de ponctuation, des données inexactes associées à un champ, des données incomplètes ou désuètes, ou même des données inscrites en double dans la base de données. Le nettoyage des données sert à corriger la situation].

5.4 Expérience dans l'intégration de solutions de GIJIA dans de grandes organisations

Quelle est l'expérience de votre entreprise dans l'intégration de solutions de GIJIA dans une grande organisation? Pourriez-vous résumer le processus d'intégration utilisé?

5.5 Expérience dans l'exécution de solutions de GIJIA automatisées

Quelle est l'expérience de votre entreprise dans l'élaboration et le déploiement de solutions de soutien pour l'automatisation des fonctions de GIJIA? Pourriez-vous résumer votre expérience dans les processus suivants :

- 5.5.1 Activités automatisées :
 - 5.5.1.1 d'approvisionnement;
 - 5.5.1.2 de retrait;
 - 5.5.1.3 de gestion d'un profil utilisateur en libre-service;
 - 5.5.1.4 de détection des anomalies;
 - 5.5.1.5 de flux de travail et d'approbation;
 - 5.5.1.6 tout autre exemple pertinent.

5.6 Expérience dans l'exécution de solutions de GIJA dans des domaines et des niveaux de sécurité des réseaux variés

Actuellement, les Forces armées canadiennes (FAC) et le MDN utilisent de nombreux domaines d'information et de sécurité répartis selon des niveaux organisationnels (stratégiques, opérationnels et tactiques) et des classifications de sécurité multiples (Très secret, Secret, Confidentiel, Protégé). Résumez votre expérience dans la réalisation de solutions dans des environnements assortis de domaines et de classifications de sécurité variés?

5.7 Renseignement de GIJA

Quelles solutions de renseignement de GIJA votre entreprise peut-elle fournir pour aider le Ministère à atténuer les cybermenaces? Voici les domaines du renseignement auxquels s'intéresse le MDN :

- 5.7.1 Surveillance en temps réel des autorisations d'accès des utilisateurs;
- 5.7.2 Surveillance en temps réel des demandes d'accès des utilisateurs;
- 5.7.3 Identification des comptes orphelins, notamment le nombre de comptes actifs et inactifs, la date de la dernière utilisation et les données consultées;
- 5.7.4 Identification des accès normaux par rapport aux accès suspects.

5.8 Risques

1.9.1. D'après votre expérience, quels risques ont été pris en compte au moment de la mise en œuvre de votre solution?

1.9.2 Qu'avez-vous fait pour atténuer ces risques?

1.10 Sécurité et protection des renseignements personnels

1.10.1 La sécurité des renseignements et la protection de la vie privée dès l'étape de la conception constituent une priorité du MDN et des FAC. Quelle approche ou conception votre entreprise a-t-elle adoptée pour assurer la sécurité des renseignements traités dans le cadre de votre solution et comment protège-t-elle la vie privée d'une personne?

1.10.2 La clé de la mise en œuvre d'une solution de GIJA au MDN est la capacité de soutenir divers niveaux d'assurance de l'identité et des justificatifs. Quelle est l'expérience de votre entreprise dans la mise en œuvre de services et de processus opérationnels qui appuient l'assurance de l'identité et des justificatifs jusqu'au niveau quatre inclusivement?

1.11 Interopérabilité

1.11.1 Le MDN et les FAC a recours à de nombreux systèmes, services, domaines, applications et partenaires, dont certains ont des exigences en matière d'interopérabilité différentes. Quelle approche adopteriez-vous pour vous assurer que les solutions de GIJA conviennent pour le MDN et les FAC et pour d'autres ministères et agences du gouvernement et partenaires multinationaux, notamment en ce qui a trait aux exigences d'interopérabilité entre les solutions de GIJA actuelles et à venir?

1.11.2 La fédération des services de GIJIA entre des partenaires est-elle une solution viable?

1.11.3 Avec quelles normes d'interopérabilité liées à la GIJIA (le cas échéant) votre solution est-elle en conformité?

1.12 Approche d'exécution recommandée

1.12.1 D'après votre expérience de mise en œuvre de solutions de GIJIA, quelle approche adopteriez-vous pour exécuter les solutions de GIJIA dans l'environnement du MDN et des FAC (p. ex. nouvelle approche, logiciels commerciaux [COTS] ou solution conçue sur mesure à partir de systèmes actuels, prestation de l'ensemble ou de certaines des fonctions de GIJIA « comme service », autre approche ou combinaison d'approches)?

1.12.2 Pourquoi proposez-vous cette approche?

1.13 Questions recommandées pour une demande de renseignements (DDR)

En tenant compte de votre expérience en GIJIA, quels types de questions suggèreriez-vous pour la DDR et quels renseignements supplémentaires souhaiteriez-vous connaître pour mieux formuler vos réponses à propos de solutions possibles et de coûts associés?

1.14 Questions sur l'engagement de l'industrie – retombées industrielles et technologiques (RIT) et proposition de valeur (PV) de la GIJIA :

Secteur de la défense

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

1.14.1 Compte tenu du niveau élevé des exigences obligatoires que propose le MDN, veuillez décrire les activités de travail direct que votre entreprise s'engagerait à entreprendre au Canada pour la production et l'entretien de la GIJIA. Dans votre réponse, veuillez préciser quelles activités de travail direct votre entreprise envisagerait de réaliser au Canada dans le domaine de la capacité industrielle clé (CIC) de cyberrésilience.

Développement des sources d'approvisionnement

La Politique des RIT vise à améliorer la compétitivité de l'industrie canadienne en encourageant sa participation et en intensifiant la présence d'entreprises, y compris les petites et moyennes entreprises (PME).

1.14.2 Dans le contexte du projet de GIJIA, veuillez préciser les nouvelles occasions qui pourraient être offertes aux fournisseurs canadiens dans la chaîne d'approvisionnement et les occasions qui pourraient spécifiquement cibler les PME (moins de 250 employés au Canada). Veuillez inclure dans votre réponse les renseignements concernant :

- a. Les activités qui devraient être perçues comme apportant la plus grande valeur au Canada et quelle incidence elles devraient avoir sur les fournisseurs canadiens;
- b. Les possibilités de développement de sources d'approvisionnement dont on pourrait profiter dans la CIC de cyberrésilience, directement ou indirectement liées au projet de GIJIA.

1.14.3 La Politique des RIT exige qu'au moins 15 % de la valeur du contrat soit attribuée à des PME canadiennes. Veuillez décrire les défis et les possibilités que vous envisagez si le Canada encourage une participation accrue des PME en faisant appel à une exigence cotée.

Perfectionnement des compétences et formation

La Politique des RIT favorise l'établissement et le maintien d'une force de travail canadienne diversifiée, talentueuse et novatrice grâce à un accès à la formation, à la sensibilisation, à l'offre de possibilités et à la prestation de programmes.

1.14.4 Quels types d'investissements en matière de perfectionnement des compétences et de formation offriraient le plus d'avantages pour le Canada (secteurs de la défense ou commercial)?

- a. Exemples :
- i. Programmes d'apprentissage intégré au travail (p. ex., enseignement coopératif; placements en milieu de travail);
 - ii. Programmes d'apprentissage;
 - iii. Un programme de perfectionnement des compétences nouveau ou actuel offert dans un établissement d'enseignement postsecondaire, ou par l'entremise de celui-ci (p. ex. codage et programmation, ingénierie des réseaux ainsi que développement et intégration de logiciels);
 - iv. Prise en charge des attestations de sécurité (p. ex. : « Très secret », International Traffic in Arms Regulations [ITAR]) ou des attestations de conformité en matière de cybersécurité pour les entreprises canadiennes, en particulier les PME.

1.14.5 Veuillez décrire les activités de perfectionnement des compétences et de formation actuellement réalisées par votre entreprise et comment l'entreprise pourrait mettre ces activités au service des Canadiens. Dans votre réponse, veuillez préciser les activités de perfectionnement des compétences et de formation qui sont liées actuellement à la CIC de cyberrésilience, ou pourraient le devenir.

Recherche et développement (R-D)

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

1.14.6 Veuillez décrire les domaines prioritaires pour les investissements en R-D et en quoi ils sont liés au projet de GIJA. Dans votre réponse, veuillez préciser dans quelle mesure ces domaines prioritaires s'arriment à la CIC de cyberrésilience.

1.14.7 Compte tenu du rôle que jouent les établissements d'enseignement postsecondaire et les instituts de recherche du secteur public pour favoriser l'innovation au Canada, veuillez décrire les possibilités directes ou indirectes que votre entreprise envisage d'entreprendre au Canada avec ces organismes et les domaines dans lesquels vos recherches seraient menées.

1.14.8 Est-il possible d'investir dans des partenariats de recherche et de développement avec des PME et des entreprises de démarrage canadiennes, y compris le financement de la R-D de stade tardif et la commercialisation de produits ou de services innovants?

Exportation

La Politique des RIT favorise la capacité des entreprises canadiennes, y compris les PME, à exploiter avec succès les marchés d'exportation, augmentant ainsi leur productivité et leur compétitivité sur le marché mondial.

1.14.9 Veuillez décrire les possibilités d'exportation en provenance du Canada directement liées à ce processus d'approvisionnement.

1.14.10 Est-il possible de garantir des droits de propriété intellectuelle suffisants et un mandat de production mondiale exclusif pour exporter dans le cadre de vos opérations canadiennes, y compris les filiales et les partenaires de la chaîne d'approvisionnement?

1.14.11 Veuillez décrire toutes les occasions d'exportation de grande valeur du Canada liées à des applications plus larges de la cybersécurité, qu'elles soient commerciales ou de défense, qui peuvent être exploitées à la suite de cette acquisition.

Autres questions

1.14.12 Veuillez indiquer, le cas échéant, les autres CIC pertinentes qui s'arriment aux travaux à exécuter relativement au projet de GIJIA? Veuillez préciser quelles CIC devraient être considérées et pourquoi elles devraient l'être. Dans votre réponse, veuillez décrire comment les CIC proposées amélioreraient les possibilités que la PV pourrait entraîner pour l'industrie canadienne.

1.14.13 Comparativement au prix et au mérite technique, la PV a généralement une pondération de 10 % de la note globale de la soumission. Que pensez-vous de la pondération de la PV pour le projet de GIJIA?

1.14.14 Dans la PV, quels sont vos pourcentages minimaux recommandés de pondération pour chacun des piliers de la proposition de valeur (défense, développement des sources d'approvisionnement, compétences et formation, R-D et exportation)?

Veuillez remettre vos réponses écrites et tout commentaire lié aux RIT ou à la PV à l'autorité contractante de Services publics et Approvisionnement Canada (SPAC) d'ici l'échéance de la lettre d'intérêt.

ANNEXE A : CAPACITÉ ET PROJET DE GESTION DE L'IDENTITÉ, DES JUSTIFICATIFS D'IDENTITÉ ET DE L'ACCÈS (GIJIA)

1. INTRODUCTION :

- 1.1. Le projet de GIJIA permettra d'améliorer l'accessibilité pour l'ensemble des organisations, d'atténuer les risques pour la sécurité des installations, des renseignements et des technologies de l'information (TI) et de réduire les contraintes sur la productivité attribuables aux problèmes relatifs aux contrôles de l'accès au MDN, avec d'autres ministères et agences du gouvernement et avec des partenaires multinationaux, notamment les États-Unis, l'Organisation du traité de l'Atlantique Nord (OTAN) et le Groupe des cinq.
- 1.2. La nouvelle approche de GIJIA au Ministère protégera les biens, uniformisera la capacité d'accès aux ressources des utilisateurs, améliorera la prise de décisions relatives à l'octroi et au retrait des droits d'accès et atténuera les risques de pertes, de dommages et de compromissions pour les biens ministériels.

2. FACTEURS OPÉRATIONNELS DE LA GIJIA

- 2.1. Facteurs gouvernementaux. Les caractéristiques de la capacité de GIJIA du MDN sont fondées sur l'orientation législative canadienne, qui exige ce qui suit : (1) l'information et les biens de technologie de l'information (TI) du gouvernement du Canada doivent être sécurisés et (2) les renseignements permettant d'identifier une personne doivent être protégés et soumis à un contrôle¹. Pour que la capacité de GIJIA respecte les lois, le MDN aura recours à la Stratégie sur la sécurité de la technologie de l'information de la Défense², qui décrit les éléments d'un environnement de sécurité intégrée, notamment l'application de la politique de sécurité, de l'authentification, du contrôle de l'accès, du compte rendu et de la vérification.
- 2.2. Technologie. Les avancées technologiques ont rendu les capacités de GIJIA plus efficaces. La GIJIA pourra tirer profit des technologies comme la biométrie, la chaîne de blocs, l'authentification à facteurs multiples, la segmentation en unités et la cryptographie moderne pour renforcer l'authentification et l'autorisation, et permettre le contrôle d'accès basé sur les attributs à la fois des actifs informationnels physiques et électroniques.
- 2.3. Cybermenace. Les technologies émergentes permettent un accès aux renseignements plus large et plus facile. Alliées à des menaces criminelles, de renseignement et militaires de plus en plus sophistiquées et tenaces, ces nouvelles technologies augmentent les risques d'accès non autorisé à des renseignements électroniques et à des biens matériels.
- 2.4. Efficacité. Avec le temps, le MDN tire de plus en plus profit de la TI en tant que catalyseur opérationnel. Initialement, les systèmes, les réseaux, les applications et les dépôts d'utilisateurs associés étaient déployés de façon indépendante surtout en raison des contraintes de sécurité ou techniques au moment de la mise en œuvre du système. L'infrastructure de TI a évolué de sorte que la convergence et l'interopérabilité des systèmes et des environnements sont nécessaires pour assurer l'efficacité opérationnelle du MDN et des FAC. Les systèmes cloisonnés actuels peuvent tirer profit d'une capacité commune de GIJIA pour permettre l'application de la stratégie de convergence de l'infrastructure de TI.

¹ Règlement sur la protection des renseignements personnels DORS/83-508 (<https://laws-lois.justice.gc.ca/fra/reglements/DORS-83-508/page-1.html>).

² Stratégie sur la sécurité de la technologie de l'information de la Défense, 8 juin 2010 (<http://admm-smagi.mil.ca/fr/a-propos/gouvernance/documents-cles.page>).

- Le Ministère espère que la GIJA améliorera l'efficacité des façons suivantes:
 - a. Adopter des normes pour les données d'identité;
 - b. Tirer parti des technologies émergentes comme la biométrie;
 - c. Rationaliser les processus opérationnels manuels actuels grâce à l'automatisation;
 - d. Améliorer l'expérience de l'utilisateur et réduire le nombre de comptes d'accès.

2.5 Confidentialité. La GIJA protégera les renseignements personnels et la confidentialité de l'information.

3. DESCRIPTION DE LA CAPACITÉ

3.1. Le projet de GIJA étudiera des solutions ministérielles pour l'approvisionnement, la gestion et le retrait des comptes et des droits d'accès pour les réseaux, les applications, les services de TI et les systèmes de contrôle des installations.

3.2. Le Ministère envisage d'adopter une architecture de GIJA conceptuelle, comme l'illustre la figure 1. À noter que cette architecture comprend ce qui suit : gestion de l'identité, gestion des justificatifs, gestion de l'accès, compte rendu, vérification et fédération³.

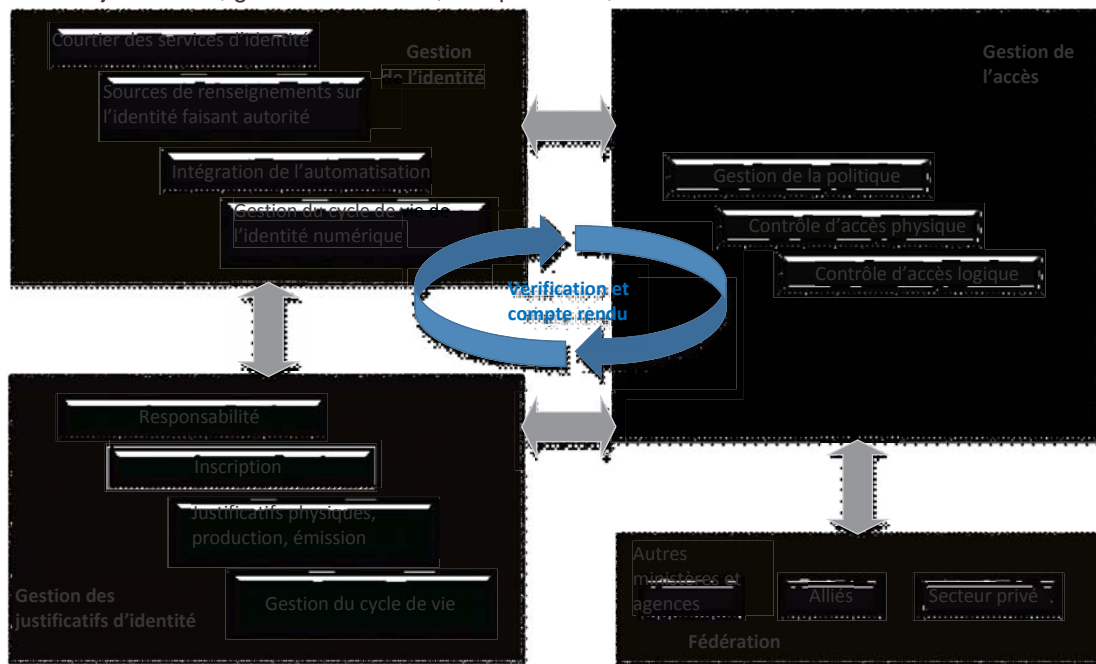


Figure 1: Architecture de GIJA conceptuelle du MDN

4. Description du projet

4.1. Un projet de GIJA pour le MDN a été établi et approuvé. Le projet fournira des capacités de GIJA, notamment une structure, une gouvernance, de la documentation, une infrastructure et de la formation organisationnelles, afin d'améliorer la capacité du Ministère à gérer l'identité, les justificatifs d'identité et les contrôles d'accès de façon coordonnée.

³ En TI, la gestion fédérée de l'identité correspond à l'adoption de politiques, de pratiques et de protocoles communs pour gérer l'identité et la confiance dans les utilisateurs de TI et les appareils dans l'ensemble des organisations.

4.2. Actuellement, le projet en est à la phase d'analyse des options qui permet d'étudier les options d'exécution de la capacité. L'analyse des options tient compte de l'efficacité, du coût, de l'échéancier et de la faisabilité technique. À la fin de cette phase, l'équipe du projet préparera une analyse de rentabilisation détaillée qui sera présentée au Comité des capacités de la Défense pour l'aider à décider si le projet doit être maintenu et s'il doit passer à la phase de définition. Le projet devrait être livré d'ici 2022 à 2027.

5. OPTIONS DE MISE EN ŒUVRE ENVISAGÉES

5.1. Les options suivantes sont envisagées et tous les commentaires concernant ces options sont les bienvenus.

- Améliorer les systèmes de GIJA actuels, en ajoutant des éléments de gouvernance, des processus opérationnels et une certaine intégration technique aux systèmes actuels;
- Fournir de nouveaux services de GIJA centralisés, dont un répertoire d'identité contenant ou utilisant des sources de renseignements sur l'identité faisant autorité déjà en usage au Ministère;
- En s'appuyant sur l'option 2, créer un courtier des services d'identité pour faciliter l'échange de renseignements sur l'identité entre les dépôts décentralisés, les systèmes de délivrance, les systèmes de contrôle d'accès et les utilisateurs.