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

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

**Gatineau**
**Québec**
**K1A 0S5**
**Bid Fax: (819) 997-9776**

# LETTER OF INTEREST
# LETTRE D'INTÉRÊT

**Title - Sujet**
Solution Nationale en Matiere de Cy

| **Solicitation No. - N° de l'invitation** | **Date** |
|---|---|
| M7594-200151/A | 2019-06-05 |
| **Client Reference No. - N° de référence du client** | **GETS Ref. No. - N° de réf. de SEAG** |
| M7594-200151 | PW-$$XL-126-35782 |
| **File No. - N° de dossier** | **CCC No./N° CCC - FMS No./N° VME** |
| 126xl.M7594-200151 | |

**Solicitation Closes - L'invitation prend fin**
**at - à 02:00 PM**
**on - le 2019-06-21**

**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:** | **Buyer Id - Id de l'acheteur** |
|---|---|
| Martyniuk, David | 126xl |
| **Telephone No. - N° de téléphone** | **FAX No. - N° de FAX** |
| (613) 402-0570 ( ) | ( ) - |

**Destination - of Goods, Services, and Construction:**
**Destination - des biens, services et construction:**
David.martyniuk@tpsgc-pwgsc.gc.ca

**Comments - Commentaires**

**Instructions: See Herein**

**Instructions: Voir aux présentes**

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

| **Delivery Required - Livraison exigée** | **Delivery Offered - Livraison proposée** |
|---|---|
| See Herein | |

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

**Telephone No. - N°de téléphone**
**Facsimile No. - N° de télécopieur**

**Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)**
**Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)**

**Signature** **Date**

**Issuing Office - Bureau de distribution**
Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Canada

# DEMANDE DE RENSEIGNEMENTS CONCERNANT UNE SOLUTION NATIONALE EN MATIÈRE DE CYBERCRIMINALITÉ

## TABLE DES MATIÈRES

# DEMANDE DE RENSEIGNEMENTS CONCERNANT UNE SOLUTION NATIONALE EN MATIÈRE DE CYBERCRIMINALITÉ POUR LA GENDARMERIE ROYALE DU CANADA (GRC)

## 1) Contexte et objet de la présente demande de renseignements (DDR)

En 2015, le ministre de la Sécurité publique et de la Protection civile a dirigé « un examen des mesures en place pour assurer la protection des Canadiens et des infrastructures critiques du Canada contre les cybermenaces ». L'examen a conclu que le Canada a besoin d'un mécanisme national pour coordonner les opérations d'application de la loi contre les cybercriminels et d'un cadre national permettant aux citoyens et aux entreprises du Canada de signaler les cybercrimes à la police.

À l'heure actuelle, les organismes d'application de la loi réagissent aux cybercrimes de manière isolée et au cas par cas à l'échelle locale. Ils ne sont pas en mesure d'établir des liens et d'évaluer les vastes répercussions de la cybercriminalité sur les victimes et la macroéconomie.

L'objectif de la présente DDR consiste à demander à l'industrie des informations sur l'énoncé concis du problème présenté ici, dans un format de défi.

### a. Mandat de l'Unité nationale de coordination de la lutte contre la cybercriminalité

La cybercriminalité est souvent peu signalée, car les mécanismes de signalement peuvent prêter à confusion pour le public canadien. Le mandat de l'Unité nationale de coordination de la lutte contre la cybercriminalité consiste à :

- Faciliter la coordination et la synchronisation des enquêtes en matière de cybercrimes au Canada et éviter les conflits entre ces dernières, ainsi que faciliter la collaboration avec les partenaires internationaux.
- Prodiguer des conseils et des avis sur les enquêtes touchant le numérique aux organismes canadiens d'application de la loi.
- Produire du renseignement « utilisable » sur les cybercrimes à l'intention des organismes canadiens d'application de la loi.
- Exploiter un système de signalement de la cybercriminalité à l'intention des citoyens et des entreprises du Canada.

### b. La situation actuelle

Le Canada ne dispose pas d'un centre de coordination national pour les efforts d'application de la loi concernant la cybercriminalité. À l'heure actuelle, les organismes canadiens

d'application de la loi réagissent aux cybercrimes de façon isolée et au cas par cas au niveau local; ils n'ont pas la capacité de tirer des conclusions et d'évaluer les répercussions macroéconomiques et les répercussions sur les victimes de la cybercriminalité et de réagir en conséquence. Cette lacune entraîne des inefficacités et un dédoublement des efforts. La cybercriminalité est souvent signalée en partie et il existe de nombreux mécanismes de signalement qui sèment la confusion chez le public, les entreprises et les victimes de la cybercriminalité. Le Canada n'a pas de mécanisme national visant à améliorer la façon dont les entreprises et le public signalent les incidents de cybercriminalité aux organismes d'application de la loi.

En vue d'atteindre l'état cible, la GRC élabore actuellement un site Web public, à titre de solution nationale à la cybercriminalité, qui permettra aux citoyens et aux entreprises du Canada de signaler les cybercrimes. Ce système de signalement de la cybercriminalité est une composante de la solution finale de l'Unité NC3, mais il ne fait pas partie du champ d'application de la présente DDR.

### c. L'état cible

Le Canada veut donner aux citoyens canadiens et aux organismes d'application de la loi canadiens un accès à des renseignements adéquats, intégrés et dans un délai convenable aux fins d'une prise de décisions précises et stratégiques.
La solution cible doit comprendre des processus et des flux opérationnels, un échange et un flux d'information ainsi qu'une catégorisation et une évaluation de l'information par des règles opérationnelles et des analyses.

Conformément aux exigences de l'état cible, l'Unité de coordination de la lutte contre la cybercriminalité nécessite l'accès à un dépôt de données centralisé, structuré et non structuré, pour le stockage et la récupération sécurisés d'informations numériques de tailles et de types différents et de métadonnées connexes, permettant ainsi la croissance des données sans perte de performance.

Les partenaires d'exécution de la loi de la GRC devront également avoir accès à un portail sécurisé afin d'obtenir ou de fournir des renseignements. La solution devrait fournir un service aux partenaires permettant ainsi de repérer les maliciels et d'agir comme intermédiaire pour de telles demandes, c'est-à-dire, recevoir l'échantillon de maliciels, préparer un condensé numérique et déterminer si l'échantillon correspond à un enregistrement existant. La solution de l'état cible est présentée à l'annexe A.

Un certain nombre de capacités et de considérations opérationnelles sont nécessaires pour tous les aspects de la solution, comme suit :

- La capacité de traduire des textes de plusieurs langues avec un niveau élevé de précision en français ou en anglais est requise. Le système devrait s'adapter à l'utilisation de termes et d'expressions spécifiques communs aux activités criminelles, en particulier la cybercriminalité. Le processus ne peut pas modifier le document ou le fichier source de la traduction.
- La reconnaissance vocale et la transcription, au minimum en français et en anglais, sont également requises. Facultativement, diriger une traduction multilingue de plusieurs langues vers l'anglais et/ou le français.

- Pour tous les moyens de réception de l'information, le système doit conserver une copie de l'information source, ainsi que de tout document dérivé ou produit, afin de maintenir la traçabilité vers la source.
- Terminer la gestion du cycle de vie de l'information, y compris la gestion des données, les autorisations, la protection, l'archivage, la purge, entre autres. La gestion du cycle de vie doit respecter des périodes de conservation précises des renseignements gérés.
- Capacité de soutenir les algorithmes et les méthodes fondés sur l'intelligence artificielle (IA) et l'apprentissage automatique (AA) dans le traitement et l'analyse des mégadonnées.
- Suivre et consigner, dans un fichier du journal, les activités de tous les utilisateurs et les interactions des utilisateurs, y compris les activités du système. Un journal de vérification non modifiable de toutes les activités pertinentes des utilisateurs et des systèmes doit être créé et conservé.

Les fonctionnalités proposées doivent être alignées, évolutives et permettre une intégration compatible avec les systèmes et applications techniques internes de la GRC

## 2) Nature de la demande de renseignements

Cette DDR est une initiative consultative par laquelle la Gendarmerie royale du Canada (GRC), ci-après dénommée le Canada, demande à l'industrie son point de vue sur les solutions commerciales et techniques éprouvées, y compris les leçons apprises et les pratiques exemplaires qui aideront le Canada à satisfaire aux exigences d'une solution nationale en matière de cybercriminalité. À la suite de cette DDR, le Canada peut utiliser les commentaires de l'industrie pour aller de l'avant avec une ou plusieurs demandes de propositions (DP) qui mettront l'accent sur la capacité de l'industrie à fournir la solution.

La présente DDR ne constitue pas un appel d'offres ni une demande de propositions (DP). Aucun accord ni contrat fondé sur la présente DDR ne sera conclu. Elle ne constitue nullement un engagement de la part du gouvernement du Canada, et elle n'autorise aucunement les éventuels répondants à entreprendre des travaux dont le coût pourrait être réclamé au Canada. Enfin, elle ne doit pas être considérée comme un engagement de la part du Canada à émettre une demande de soumissions subséquente ou à attribuer un contrat pour les travaux décrits dans les présentes.

La participation à cette DDR est encouragée, mais elle n'est pas obligatoire. Elle ne servira pas à dresser une liste abrégée des entreprises qui pourraient contribuer aux travaux à venir. De plus, la participation à la présente DDR n'est ni une condition ni un préalable pour participer à toute demande de soumissions subséquente.

## 3) Coûts associés aux réponses

Le Canada ne remboursera pas les dépenses engagées pour répondre à cette DDR.

## 4) Traitement des réponses

**a)** Utilisation des réponses : Les réponses ne seront pas soumises à une évaluation officielle. Toutefois, le Canada pourra les utiliser pour élaborer ou modifier ses stratégies d'acquisition ou tous documents préliminaires joints à cette DDR. Le Canada examinera toutes les réponses reçues d'ici la date de clôture de la DDR. Cependant, s'il le juge opportun, il pourrait examiner les réponses reçues après la date de clôture de la DDR.

**b)** Équipe d'examen : Une équipe d'examen composée de représentants du client (selon le cas) et de fonctionnaires de Travaux publics et Services gouvernementaux Canada (TPSGC) examinera les réponses reçues. Le Canada se réserve le droit de recourir à des experts-conseils indépendants ou aux ressources gouvernementales dont il dispose et qu'il juge nécessaires pour examiner les réponses. Toutes les réponses ne seront pas nécessairement soumises à l'examen de tous les membres de l'équipe d'examen.

**c)** Confidentialité : Les répondants devraient indiquer les parties de leur réponse qu'ils jugent de nature exclusive ou confidentielle. Le Canada traitera ces renseignements de façon confidentielle, conformément à la Loi sur l'accès à l'information.

**d)** Activité de suivi : Le Canada pourrait, à sa discrétion, communiquer avec tout répondant pour lui poser d'autres questions ou obtenir des éclaircissements quant à un aspect ou un autre d'une réponse. Le Canada pourrait également, à sa discrétion, inviter un ou plusieurs fournisseurs à présenter une démonstration de leur solution conformément à la présente DDR. L'autorité contractante mènera l'activité de suivi avec tout fournisseur à sa discrétion.

## 5) Contenu de la présente DDR

La DDR comprend aussi des questions particulières à l'intention de l'industrie.

| **Profil de l'entreprise** |
| --- |
| 1. Décrivez les qualifications et l'expertise de votre entreprise dans le domaine de la cybersécurité.<br>2. Vos offres d'affaires actuelles sont-elles harmonisées avec la stratégie numérique du gouvernement du Canada qui offre des services infonuagiques, des capacités d'intelligence artificielle, entre autres?<br>3. Votre entreprise a-t-elle travaillé avec d'autres fournisseurs afin d'élaborer une solution organisationnelle intégrée au cours des trois dernières années? Dans l'affirmative, veuillez décrire brièvement les circonstances et les résultats.<br>4. Décrivez les réalisations de votre entreprise en matière d'analyse de données au cours des cinq dernières années.<br>5. Décrivez les antécédents et l'expérience de l'entreprise en matière d'élaboration de structures, de processus et d'environnements qui favorisent la diffusion d'information et la collaboration. |

| Solution du fournisseur |
| --- |
| 6. Votre solution est-elle une application de logiciels commerciaux prêts à l'emploi (LCPE)?<br>7. Votre solution comporte-t-elle toutes les composantes décrites dans le présent document et à l'annexe A (Vue de l'état cible)? Sinon, veuillez fournir des explications concernant les lacunes fonctionnelles.<br>8. Si votre solution ne comporte pas toutes les composantes décrites dans le présent document, votre organisation est-elle disposée à avoir recours à d'autres fournisseurs, dans le cadre d'une coentreprise, afin de proposer une solution qui répondra à toutes les exigences décrites aux présentes?<br>9. Avez-vous mis en œuvre votre solution au sein d'un autre organisme au sein du gouvernement fédéral ou provincial, ou dans le secteur privé?<br>10. Votre solution comporte-t-elle actuellement une fonctionnalité d'intelligence artificielle ou de langage machine (IA/LM)?<br>11. Quels autres aspects ou quelles autres fonctionnalités recommanderiez-vous pour ajouter de la valeur à cette solution?<br>12. Votre solution fonctionne-t-elle dans les deux langues officielles du Canada (anglais, français)?<br>13. Comment la solution du fournisseur s'adapterait-elle aux changements technologiques et opérationnels futurs? Quelles options le fournisseur propose-t-il pour faire face aux changements constants des exigences opérationnelles?<br>14. D'après votre expérience, quelles sont les méthodes d'enquête cybernétiques actuelles? Laquelle recommanderiez-vous en fonction de la compréhension de nos exigences?<br>15. En vous fondant sur votre expérience, décrivez les pratiques exemplaires liées aux enquêtes et aux rapports cybernétiques (saisie DNS (Domain Name Services) / saisie de domaine / saisie de monnaie cryptographique).<br>16. Décrivez la feuille de route à venir de la solution avec les délais de diffusion prévus. |
| **Documents d'affaires et de formation** |
| 17. Selon votre expérience, quelles sont les méthodes actuelles de coordination et d'analyse des données et de l'information? Laquelle recommanderiez-vous en fonction de la compréhension de nos exigences?<br>18. Disposez-vous de documents de formation facilement accessibles pour les nouveaux utilisateurs de votre solution?<br>19. En vous fondant sur votre expérience, décrivez l'approche et les pratiques exemplaires liées à la prestation de formation en matière de coordination et d'analyse des données et de l'information. |

20. Ludification du processus d'apprentissage : décrivez votre expérience quant à la création d'un environnement virtuel où les gens peuvent apprendre et mettre en commun les pratiques exemplaires.

**Conformité technique**

21. Le matériel et les logiciels qui composent votre solution utilisent-ils les normes ISO ou d'autres normes ou y a-t-il des pièces ou composantes brevetées?
22. La GRC exige l'application d'un degré élevé de confiance envers l'identité des utilisateurs à l'aide d'une méthode d'authentification à deux facteurs. De quelle façon votre solution permet-elle une authentification à deux facteurs?
23. La GRC doit être en mesure d'extraire ses données ou de les copier à partir de la solution dans un format non exclusif et utilisable à tout moment. Dans quelle mesure votre solution satisfait-elle à ces exigences?
24. Le logiciel est-il compatible avec la technologie de pointe de l'industrie (notamment les systèmes d'exploitation, les systèmes de base de données, les appareils mobiles, les navigateurs Internet)? Veuillez fournir des détails sur les exigences minimales en matière de version.
25. Veuillez fournir des détails sur les exigences minimales en matière de version.
26. Comment et quand avez-vous été déployé dans un environnement infonuagique public? Sur quelle plateforme de fournisseur de service infonuagique votre solution a-t-elle été déployée?
27. La solution est-elle conçue selon la norme d'architecture d'entreprise ou tout autre cadre d'architecture de pointe de l'industrie?
28. La solution a-t-elle été conçue pour présenter une interface conforme au modèle NIEM pour l'échange d'information avec des systèmes externes?

**Questions pour la mise en œuvre de l'informatique en nuage**

29. La solution proposée par le fournisseur est-elle conforme aux services d'infonuagique, à l'intelligence artificielle (IA), aux capacités d'apprentissage machine (AM) et aux normes architecturales sur le numérique du gouvernement du Canada décrits aux pages suivantes : *https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/normes-numeriques-gouvernement-canada.html*; et *https://canada-ca.github.io/digital-playbook-guide-numerique/views-vues/gc-earb-ceai/fr/ceai-gc.html*
30. La GRC exige de conserver la pleine propriété de toutes ses données opérationnelles. Dans quelle mesure la solution ou le fournisseur satisfait-il à cette exigence?
31. La GRC doit évaluer le rendement, la disponibilité et la sécurité de ses solutions à l'aide de processus et d'outils internes et/ou d'outils de tierce partie. Dans quelle mesure la solution ou le fournisseur satisfait-il à cette exigence?
32. La GRC exige de la transparence pour toutes les violations de sécurité qui ont une incidence sur ses services ou ses données. Avec quelle rapidité et quelle exhaustivité le fournisseur signale-t-il ces violations?

33. La GRC exige que toutes les données soient hébergées dans des centres de données canadiens, situés dans les limites des frontières canadiennes. Dans quelle mesure votre solution satisfait-elle à ces exigences?
34. La GRC exige que toutes les activités du fournisseur en lien avec des données de la GRC soient entièrement consignées et vérifiables. Elle exige en outre nécessaire que le fournisseur obtienne une autorisation écrite de la GRC avant tout accès. Veuillez expliquer comment la solution permet de contrôler et de suivre les activités des fournisseurs.
35. La GRC peut avoir recours à un fournisseur de service IDaaS pour offrir un service d'identification externe cohérent. Dans quelle mesure pouvez-vous respecter cette exigence?
36. La GRC exigera une vérification (p. ex., facturation, utilisation, rendement de la solution, disponibilité, interruption de service) des services fournis. Quels sont les types de rapports offerts et avec quelle rapidité peuvent-ils être fournis?
37. La GRC exige que toutes les données soient chiffrées pendant le stockage et le transit. Dans quelle mesure votre solution satisfait-elle à ces exigences?
38. La GRC peut utiliser un service de gestion des clés pour le stockage et la gestion des clés de chiffrement. Dans quelle mesure pouvez-vous respecter cette exigence?

## 6) Confidentialité des réponses des fournisseurs

Même si les renseignements recueillis peuvent être fournis sous forme d'information confidentielle (dans ce cas, ils seront traités en conséquence par le Canada), le Canada peut les utiliser dans le cadre de la rédaction d'une demande de soumissions ou de documents contractuels à venir.

On invite les répondants à indiquer, dans l'information fournie au Canada, tout renseignement qu'ils considèrent comme exclusif, personnel ou appartenant à un tiers. Veuillez noter que le Canada pourrait être tenu par la loi (p. ex. en réponse à une demande en vertu de la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*) de divulguer des renseignements exclusifs ou commercialement sensibles au sujet d'un répondant.

## 7) Possibilité de séance d'information

Le Canada peut, à sa discrétion, tenir une séance d'information avec les représentants de l'industrie au sujet de la présente DDR. Le cas échéant, la date, l'heure et le lieu de la séance d'information seront diffusés ultérieurement. Si une telle séance d'information a lieu, il s'agira d'une occasion, pour les fournisseurs intéressés, de demander des clarifications au sujet de l'objectif et du contenu de la présente DDR.

## 8) Démonstration du fournisseur

Le Canada peut, à sa discrétion, tenir des démonstrations avec les représentants de l'industrie au sujet de la présente DDR. Les fournisseurs doivent exprimer par écrit leur

intérêt à fournir au Canada une démonstration de leur solution en réponse à la présente DDR. La démonstration de la solution par les fournisseurs se fera individuellement et le contenu demeurera confidentiel. La date, l'heure et le lieu des démonstrations du fournisseur seront fixés par l'autorité contractante et communiqués par écrit aux fournisseurs intéressés.

Deux scénarios qui doivent être utilisés dans la démonstration du fournisseur sont présentés dans les sections qui suivent. L'objectif est que les fournisseurs participant à la démonstration démontrent comment leur solution répond aux exigences opérationnelles énoncées dans ces scénarios.

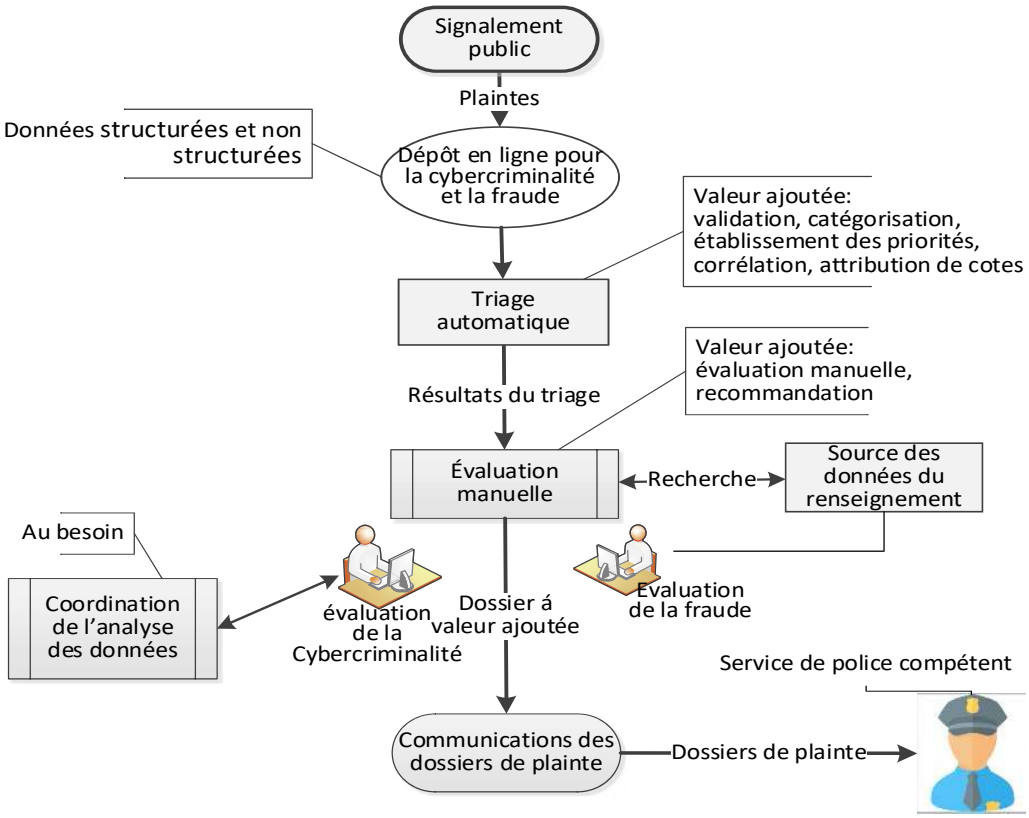
**Scénario 1 : Rapports publics**

Les rapports publics comprennent la saisie des rapports sur la cybercriminalité et la fraude provenant du public, l'intégration des rapports dans le dépôt de cybercriminalité, le triage et l'évaluation des rapports et leur diffusion aux partenaires de l'application de la loi pour qu'ils puissent faire l'objet d'une enquête plus approfondie.

La solution utilisera un processus de triage pour analyser les dossiers de plainte. Le triage déterminera si le dossier de plainte a un statut donnant lieu à une action et appliquera une note pour déterminer le traitement ultérieur. Le processus de triage peut utiliser le traitement du langage naturel pour faire des déductions et extraire des données des champs de texte ainsi que l'apprentissage automatique pour appuyer des algorithmes de notation avancés. Le processus de triage est essentiel à la priorisation des dossiers de plainte. Le triage doit être configurable pour traiter différents types de données d'entrée et contrôler les volumes nécessitant une évaluation manuelle.

L'évaluation manuelle permettra d'analyser plus à fond les dossiers de plainte traitables et d'y ajouter de la valeur avant leur diffusion à la police compétente.

Le diagramme suivant illustre le concept de rapport public :



**Scénario 2 : Réception de renseignements et demande de renseignements**

La solution recevra des données brutes, des renseignements et des présentations de renseignements ou des demandes de renseignements de divers partenaires nationaux et internationaux en matière de cybercriminalité. Ces observations peuvent être présentées pour les raisons suivantes :

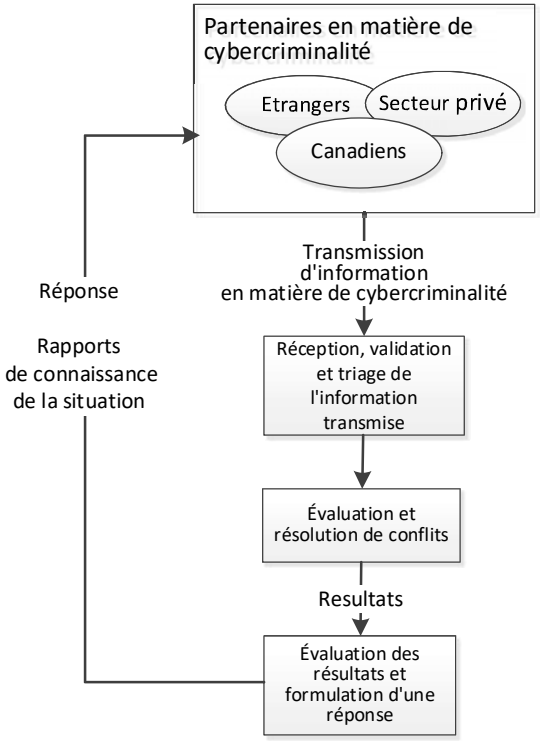
i) Requête – Y a-t-il des fonds de données liés à l'information?

ii) Information seulement – L'information est fournie à des fins de référence sur la cybercriminalité.

iii) Évaluation et réponse – Évaluer l'information fournie et retourner une réponse.

L'Unité NC3 utilisera la solution pour enregistrer la soumission, gérer le déroulement des travaux, évaluer la soumission, stocker les entités cybernétiques dans le dépôt de cybercriminalité, préparer l'information pour le traitement et effectuer toutes les activités de requête et de résolution des conflits nécessaires. La solution servira également à élaborer et à diffuser les rapports sur la connaissance de la situation qui en résultent.

Le diagramme suivant illustre le processus lié aux demandes d'information.



## 9) Format des réponses

**a)** Les répondants sont priés de fournir leurs commentaires, leurs préoccupations et, le cas échéant, leurs recommandations concernant d'autres façons de répondre aux exigences ou d'atteindre les objectifs décrits dans la présente demande de renseignements. Les répondants sont également invités à fournir des commentaires au sujet du contenu, du format ou de l'organisation de toute ébauche de document faisant partie de la présente demande de renseignements. Ils devraient expliquer toute hypothèse qu'ils présentent dans leur réponse.

**b)** **Page couverture :** si la réponse comprend plusieurs documents, le répondant doit indiquer, sur la page couverture de chacun des documents, le titre de la réponse, le numéro de la demande, le numéro du document ainsi que sa dénomination sociale complète.

**c)** **Page de titre :** la page de titre doit suivre la page couverture de chacun des documents de la réponse. Sur cette page doivent figurer :

i) le titre de la réponse et le numéro du document;

ii) le nom et l'adresse du répondant;

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

iv) la date;

v) le numéro de la DDR.

**d)** **Système de numérotation :** on demande aux répondants de préparer leurs réponses en suivant le système de numérotation employé dans la présente DDR. Toute référence à des documents descriptifs, à des manuels techniques et à des brochures accompagnant la réponse devrait respecter ce système.

**e)** **Nombre d'exemplaires :** le Canada prie les répondants de présenter un (1) exemplaire électronique de leur réponse.

## 10) Demandes de renseignements et présentation des réponses des fournisseurs

Toute question relative à la présente DDR devrait être transmise à l'autorité contractante indiquée ci-dessous. Les fournisseurs intéressés devraient adresser leur réponse à l'autorité contractante; les réponses doivent être reçues au plus tard à l'heure et à la date indiquées à la page 1 du présent document.

Autorité contractante : David Martyniuk
Courriel : David.Martyniuk@tpsgc-pwgsc.gc.ca
Téléphone : 613-402-0570

# ANNEXE A : VUE DE L'ÉTAT CIBLE