



## SERVICES PARTAGÉS CANADA

### **Demande de renseignements pour le processus d'approvisionnement concernant La Solution de surveillance d'entreprise (SSD)**

|                              |                                      |                          |                          |
|------------------------------|--------------------------------------|--------------------------|--------------------------|
| Demande de renseignements n° | [N° de la demande de renseignements] | Date                     | [Date de publication]    |
| N° de dossier GCDocs         | [N° de dossier GCDocs]               | N° de référence du SEAOG | N° de référence du SEAOG |

|   |  |   |
|---|--|---|
| Bureau émetteur   | Services partagés Canada<br>180, rue Kent, 13 <sup>e</sup> étage<br>Ottawa (Ontario) K1P 0B5 |   |
| Autorité contractante<br>(L'autorité contractante est le représentant de SPC pour tous les commentaires et toutes les questions portant sur ce document.) | Nom  | Guyline Dagenais  |
|   | N° de téléphone  | 343-542-2341  |
|   | Courriel   | guyline.dagenais@canada.ca  |
|   | Adresse postale  | 180, rue Kent, 13 <sup>e</sup> étage<br>PO Box/CP 9808 STS T CSC, Ottawa, Ontario K1G 4A8 |
| Date et heure de clôture  | 4 octobre 2019   |   |
| Fuseau horaire  | Heure avancée de l'Est (HAE)   |   |
| Destination des biens ou des services   | Sans objet – Demande de renseignements uniquement  |   |
| Courriel auquel la réponse doit être envoyée avant la date de clôture   | guyline.dagenais@canada.ca   |   |

# SERVICES PARTAGÉS CANADA

## **Demande de renseignements pour le processus d'approvisionnement concernant La Solution de surveillance d'entreprise (SSD)**

### TABLE DES MATIÈRES

|  |           |
|--|-----------|
| <b>1. RENSEIGNEMENTS GÉNÉRAUX .....</b>                              | <b>3</b>  |
| 1.1 Introduction.....  | 3         |
| 1.2 Aperçu du projet.....  | 3         |
| 1.3 Données historiques ou volumétriques.....                        | 6         |
| 1.4 Soumission de questions .....                                    | 8         |
| <b>2. RENSEIGNEMENTS DEMANDÉS PAR LE GOUVERNEMENT DU CANADA.....</b> | <b>8</b>  |
| 2.1 Commentaires au sujet des documents préliminaires .....          | 8         |
| 2.2 Réponses aux questions à l'intention de l'industrie .....        | 8         |
| <b>3. RÉPONSE DES FOURNISSEURS .....</b>                             | <b>11</b> |
| 3.1 Présentation d'une réponse .....                                 | 11        |
| 3.2 Confidentialité.....   | 11        |
| <b>4. EXAMEN DES RÉPONSES PAR LE GOUVERNEMENT DU CANADA .....</b>    | <b>11</b> |
| 4.1 Examen des réponses .....  | 11        |
| 4.2 Équipe d'examen .....  | 11        |
| 4.3 Activité de suivi.....   | 12        |

# SERVICES PARTAGÉS CANADA

## Demande de renseignements pour le processus d'approvisionnement concernant La Solution de surveillance d'entreprise (SSD)

### 1. Renseignements généraux

#### 1.1 Introduction

- a) **Phase 1 du processus d'approvisionnement** : La présente demande de renseignements (DDR) constitue la première phase d'un processus d'approvisionnement mené par Services partagés Canada (SPC) concernant La Solution de surveillance d'entreprise (SSD) (le « **Projet** »). Les fournisseurs sont invités à présenter des réponses afin d'aider le gouvernement du Canada à préciser ses exigences concernant le projet. Les fournisseurs ne sont pas tenus de présenter une réponse à la DDR pour pouvoir participer aux phases suivantes du processus d'approvisionnement concernant le projet.
- b) **L'étape de la DDR n'est pas une demande de soumissions** : La présente DDR ne constitue pas une demande de soumissions ou un appel d'offres. Aucun contrat ne sera attribué à la suite des activités tenues au cours de la présente DDR. Le gouvernement du Canada se réserve le droit d'annuler toute exigence préliminaire décrite comme faisant partie du projet à tout moment pendant la DDR ou toute autre étape du processus d'approvisionnement. Étant donné que le processus de la DDR et toute activité d'approvisionnement connexe sont susceptibles d'être partiellement ou entièrement annulés par le gouvernement du Canada, l'étape de la DDR peut ne pas aboutir à des processus d'approvisionnements subséquents.
- c) **Coûts des réponses** : SPC ne remboursera pas au fournisseur ou à ses représentants les frais généraux ou les dépenses liées à la participation aux activités de l'étape de la DDR. Il leur incombe par ailleurs d'assurer leurs propres recherches indépendantes, processus de diligence raisonnable et enquêtes ainsi que d'obtenir les conseils indépendants qu'ils jugent nécessaires et souhaitables dans le cadre de leur participation au processus de la DDR et au processus d'approvisionnement futur.

#### 1.2 Aperçu du projet

a) **Aperçu du projet :**

Le gouvernement du Canada (GC) étudie la possibilité de moderniser les procédures de surveillance de l'infrastructure et des applications dans le but :

- 1) d'améliorer notre capacité à assurer la remise en service;
- 2) d'aider notre structure de soutien à faire un meilleur travail en éliminant une partie de ses tâches routinières;
- 3) de combler les lacunes de la surveillance, grâce à une vue centralisée couvrant toute l'infrastructure et l'ensemble des applications comprises dans la portée;
- 4) de rendre proactive notre capacité de surveillance, qui a été réactive jusqu'à présent.

Services partagés Canada (SPC), qui sait fort bien qu'aucun outil n'est doté de toutes les fonctionnalités requises, privilégie l'acquisition d'un logiciel en tant que service (SaaS) pour répondre à ses besoins. Toutefois, le Ministère devra peut-être mettre en place une solution maison en raison d'impératifs touchant la sécurité. Quel que soit leur nombre, les outils choisis par SPC doivent s'interfacer avec celui de la gestion des services de technologie de l'information (GSTI) et former le système qui consigne les événements et les mesures qu'ils ont prises dans leur foulée.

À l'heure actuelle, le GC exploite des réseaux présentant diverses cotes de sécurité. Aux fins de la présente demande de renseignements, vous devez supposer que les réseaux du Ministère compris dans la portée présentent trois niveaux de sécurité, à savoir non classifié, secret et Protégé B (<https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-fra.html>).

SPC répartit la surveillance en quatre secteurs, soit :

- 1) la disponibilité, c'est-à-dire le caractère opérationnel de l'élément;
- 2) le rendement, c'est-à-dire le bon fonctionnement attendu de l'élément;
- 3) l'atténuation, c'est-à-dire l'exécution automatique d'un flux de travail en réponse à un événement;
- 4) la prévision, c'est-à-dire l'adoption d'une posture proactive qui remplace une attitude réactive.

### **Intervenants**

La Direction générale des services de centre de données (DGSCD), Réseaux, sécurité et services numériques (RSSN) et le Centre de commande d'entreprise (CCE) de la Direction générale de la prestation et de la gestion des services (DGPGS) sont les principaux utilisateurs de la solution.

### **Exigences fonctionnelles**

La présente demande de renseignements porte sur :

- 1) l'utilisation de l'intelligence artificielle (AI) pour assurer une capacité de prédire le déroulement des opérations de TI;
- 2) la gestion des événements pour maintenir la disponibilité de l'infrastructure et des applications;
- 3) l'atténuation automatique (automatisation robotisée) pour améliorer notre capacité à accélérer la remise en service;
- 4) la surveillance du rendement des applications des centres de données, actuels et d'entreprise, utilisées au service des employés fédéraux et de la population canadienne.

### **Contraintes**

Chaque réseau doit être conforme aux modalités établies dans les documents [ITSG-38](#), *Considérations de conception relatives au positionnement des services dans les zones*, et [ITSG-22](#), *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada*. La solution devrait reposer sur des serveurs de gestion des concentrateurs et des relais, déployés dans chacune des zones.

La solution doit également être conforme aux contrôles de sécurité précisés dans le document [ITSG-33](#), *Gestion des risques liés à la sécurité de la TI : Une méthode axée sur le cycle de vie*.

Application de TI essentielle, la solution de surveillance doit être hautement disponible et déployée dans plusieurs sites pour être maintenue opérationnelle dans l'éventualité où l'un d'eux tomberait en panne.

De plus, on s'attend à ce que l'outil de GSTI utilisé par SPC constitue le système de consignation de tout événement détecté et des mesures d'atténuation qui s'ensuivent.

### **Disponibilité**

Toutes les alertes sont dirigées vers le Centre de commande d'entreprise (CCE), présent dans plusieurs installations, et les alertes de surveillance sont acheminées vers des équipes particulières. Le GC a investi d'importantes ressources dans des outils de surveillance et ne prévoit pas de remplacer rapidement ces derniers. Il envisage toutefois un modèle hybride regroupant de nouveaux outils de surveillance, avec ou sans agent, au point terminal, et l'acheminement de ses consoles principales vers la nouvelle solution.

### **Rendement**

Les clients de SPC lui demandent d'assurer un service de surveillance du rendement des applications (SRA) opérationnelles. Pour y parvenir, le Ministère doit être en mesure d'effectuer un relevé des compteurs de rendement de l'infrastructure et des paramètres des applications. Il poursuit ses activités de migration des charges de travail et suit un plan pluriannuel de la migration des applications vers des centres de données d'entreprise. SPC estime avoir besoin d'un amalgame d'outils de SRA pour assurer le soutien technique des centres de données, actuels ou d'entreprise.

### **Automatisation robotisée**

SPC effectue encore des activités de soutien pour le compte de certains partenaires, activités nécessaires avant sa création. Diverses équipes réunissant des experts en la matière (EM) ont conçu des scripts permettant d'automatiser des tâches, alors que d'autres continuent d'employer des méthodes manuelles. SPC souhaite réduire les délais de remise en service et recourir à des technologies d'automatisation pour améliorer la qualité de l'exécution. SPC croit que, grâce à ces technologies, les EM auront plus de temps à consacrer à l'innovation, et que de meilleurs services seront offerts à ses partenaires. Ces technologies doivent s'interfacer avec nos outils de GSTI sous la forme d'un système de consignation. Elles doivent non seulement soutenir nos plateformes informatiques, mais également permettre le réglage des paramètres des réseaux, des ressources de stockage et des applications.

### **Solution proactive**

La technologie que gère SPC est en voie de délaisser les ressources traditionnelles de calcul, de réseau et de stockage au profit de l'infonuagique, des microservices et de l'Internet des objets. Pour parer aux difficultés que posent les volumes colossaux de données structurées et non structurées, l'apprentissage machine permet de regrouper les données et, par conséquent, de réaliser des gains de disponibilité et de rendement. L'analytique et l'apprentissage automatique (AA) permettent à SPC de surveiller en temps réel l'état de l'environnement pris en charge. Le Ministère constate que l'AA est capable de comprendre le cycle opérationnel et de faire en sorte que la surveillance ne soit plus réactive comme à l'habitude mais repose plutôt dorénavant sur la télémétrie pour établir une base de référence dynamique. Le corpus des connaissances, généré par l'analyse des causes fondamentales, ne sera plus constitué d'un ensemble hétéroclite de dépôts de documents, mais intégré à la solution recherchée, permettant ainsi à la technologie d'appuyer le processus décisionnel.

### **Interface avec les outils de surveillance**

Les clients autorisés doivent être capables de modifier les règles de surveillance de leur infrastructure et de leurs applications par l'intermédiaire d'un portail. La solution doit fonctionner dans les deux langues officielles (le français et l'anglais) et sélectionner

automatiquement celle du poste de travail de l'utilisateur. Les données s'affichent sous la forme d'un tableau de bord permettant de prendre connaissance de la situation sans avoir à le programmer. Le tableau de bord fonctionne en temps réel et accepte l'information sur la gestion des événements, l'IA et l'AM, ainsi que les données des journaux système et celles des outils de rendement des applications. La solution doit produire des formes que l'intervenant structure à sa convenance à partir de données télémétriques provenant de diverses sources.

La solution doit s'intégrer à la plateforme Active Directory aux fins d'authentification des utilisateurs et des administrateurs.

### **Intégration des outils de GSTI**

SPC a attribué un contrat pour un nouvel outil de GSTI avec lequel doit s'interfacer la solution de surveillance :

- 1) l'outil de GSTI constitue le système qui consigne tous les incidents;
- 2) la gestion des événements doit étayer les données à leur sujet en interrogeant la base de données de gestion de la configuration (BDGC) à même l'outil de GSTI.

### **Hypothèses**

Le fournisseur doit supposer que SPC dispose :

- 1) d'un réseau étendu redondant, auquel un fournisseur lui donne d'accès, ainsi que de connexions redondantes à chacun des emplacements où se trouvent des serveurs.

#### **b) Portée du processus d'approvisionnement prévu**

- i) **Utilisateurs clients potentiels** : La présente DDR est publiée par SPC. SPC prévoit utiliser le ou les contrat(s) obtenus à la suite d'une demande de soumission subséquente pour fournir des services partagés à un ou à plusieurs de ses clients. Les clients de SPC comprennent SPC lui-même, les institutions fédérales pour qui ses services sont obligatoires à tout moment pendant la durée de l'instrument subséquent, ainsi que les autres organisations qui, sur une base facultative, choisissent de recourir à ses services de temps en temps, à tout moment pendant la durée de l'instrument subséquent. Tout processus d'approvisionnement subséquent n'empêchera pas SPC d'avoir recours à une autre méthode d'approvisionnement pour ses clients qui ont des besoins identiques ou semblables, à moins qu'une demande de soumission subséquente concernant ce projet indique expressément le contraire.
  - ii) **Nombre de contrat(s)** : Le gouvernement du Canada envisage actuellement d'attribuer un contrat.
  - iii) **Durée des contrat(s) subséquents** : Le gouvernement du Canada envisage actuellement d'attribuer un contrat d'une durée de sept ans, plus deux périodes d'options de deux ans chacune.
- c) **Exception au titre de la sécurité nationale** : Le gouvernement du Canada a invoqué l'exception au titre de la sécurité nationale (ESN) à l'égard de la présente demande et, par conséquent, aucun des accords commerciaux ne s'applique à ce besoin.
  - d) **Préférence à l'égard des biens et des services canadiens** : Pour cette demande, une préférence peut être accordée aux produits ou aux services canadiens. Ces préférences seront décrites dans les demandes de soumission subséquentes.

## **1.3 Données historiques ou volumétriques**

Les exemples de données d'inventaire suivant ont été transmis aux fournisseurs afin de les aider à mieux comprendre les exigences du gouvernement du Canada. En incorporant ces données dans la présente demande de renseignements, le gouvernement du Canada ne s'engage pas à ce que l'achat ou son utilisation future de licences corresponde à ces données. Ces données sont fournies strictement à titre informatif. Bien qu'elles représentent la meilleure information que possède SPC, le gouvernement du Canada ne garantit pas qu'elles soient complètes ou exemptes d'erreurs.

| Catégorie          | Nombre d'unités | Description   |
|--------------------|-----------------|---|
| Wi-Fi              | 80 000          | Points d'accès  |
|                    | 16 000          | Systèmes sans fil de détection des intrusions   |
| Réseau             | 19 000          | Commutateurs d'accès  |
|                    | 6 000           | Commutateurs d'extrémité  |
|                    | 4 000           | Routeurs  |
|                    | 75              | Équipements optiques de SRMP (service de réseaux métropolitains partagés)   |
| Centres de données | 5 000           | Dispositifs pare-feu/Nexus, systèmes de détection des intrusions sur hôte (SDIH), systèmes de détection des intrusions sur réseau (SDIR) et dispositifs de surveillance des réseaux |
|                    | 50 000          | Serveurs virtuels (Linux/Unix/Windows)  |
|                    | 3 000           | Serveurs physiques (Linux/Unix/Windows, ressources de calcul haute performance)   |
| Stockage           | 1 000           | Réseaux de stockage, stockage en réseau, dispositifs à bandes magnétiques   |
| Stockage           | 30              | Pétaoctets  |
| Ordinateur central | 25              | Environ 10 partitions logiques (LPAR) par ordinateur central  |
|                    | 1 000           | Applications d'ordinateur central   |
| Édifices           | 102             | Centres de données, actuels et d'entreprise   |
|                    | 1 800           | Bâtis, cartes d'accès, systèmes de chauffage, de ventilation et de conditionnement de l'air (CVCA), alimentation électrique, caméras  |
| Applications       | 20 000          | Applications maison, gratuites, SAP, PeopleSoft etc.  |
| Bases de données   | 5 000           | MS SQL, Oracle, DB2, Sybase   |
| Instances Web      | 7 500           | Internet Information Services (IIS), Apache, WAS  |
| Infonuagique       | 3               | Nuage public  |
| Infonuagique       | 2               | Nuage privé   |

### Principaux outils de SPC

- Unified Infrastructure Management (UIM), Application Performance Management (APM) et Spectrum de Computer Associates
- Tivoli d'IBM

- WhatsUp Gold
- Systems Insight Manager de Hewlett-Packard
- SolarWinds
- System Center Operations Manager de Microsoft
- Nagios
- Patrol de BMC

## 1.4 Soumission de questions

- Les questions portant sur la DDR peuvent être envoyées à l'autorité contractante par courriel à l'adresse figurant sur la page de couverture au plus tard 5 jours ouvrables avant la date et l'heure limites indiquées sur la page de couverture du présent document. Le gouvernement du Canada peut ne pas répondre aux questions reçues après cette date.
- Pour garantir l'uniformité et la qualité des renseignements communiqués aux fournisseurs, les questions importantes reçues ainsi que leurs réponses seront publiées dans le Service électronique d'appels d'offres du gouvernement (SEAOG) sous forme d'une modification de la présente DDR.

## 2. Renseignements demandés par le gouvernement du Canada

### 2.1 Commentaires au sujet des documents préliminaires

Tous les documents indiquant les exigences du gouvernement du Canada relatives au présent projet qui sont remis aux fournisseurs au cours du processus de DDR ne sont que des exigences préliminaires ou des ébauches de celles-ci et pourraient changer. Ces exigences, ou une partie de celles-ci pourraient être mises à jour avant ou pendant toute demande de soumissions subséquente.

Les fournisseurs sont invités à formuler des commentaires, à faire part de leurs préoccupations et, le cas échéant, faire des suggestions sur la façon de répondre aux exigences ou d'atteindre les objectifs décrits pour le projet. Les fournisseurs sont également invités à fournir leurs commentaires sur le contenu, la forme et la manière dont l'information est structurée dans les ébauches de documents fournies avec la présente DDR. Les fournisseurs doivent expliquer les hypothèses qu'ils avancent dans leur réponse.

### 2.2 Réponses aux questions à l'intention de l'industrie

Le gouvernement du Canada demande des réponses aux questions suivantes :

- Dans l'optique de limiter la multiplication des serveurs de relais et de concentrateurs dans chaque zone, pourriez-vous fournir des renseignements détaillés au sujet de solutions possibles reposant sur l'utilisation de conteneurs ou de microservices?
- Quelles sont les différentes possibilités d'hébergement de la ou des solutions proposées pour garantir que les données demeureront au Canada (logiciel en tant que service [SaaS], infrastructure en tant que service [IaaS], plateforme en tant que service [PaaS], instances sur place, etc.)?
  - À quel taux de disponibilité et à quels objectifs touchant les points de récupération et le temps de reprise peut-on s'attendre d'un SaaS?
  - Solution SaaS
    - Comment entendez-vous protéger les renseignements personnels et la confidentialité?
    - De quelle façon la solution envisagée assure-t-elle la sécurité de la TI?



- c) Quels mécanismes ou processus prévoyez-vous pour :
- (1) empêcher l'accès sans autorisation aux données ou la compromission de leur intégrité?
  - (2) consigner et vérifier les événements utilisateurs, les modifications apportées aux règles ou aux algorithmes, ainsi que les décisions algorithmiques de la solution d'IA?
  - (3) assurer le contrôle de l'accès, en précisant son niveau de granularité (champ, dossier, décision, etc.)?
  - (4) protéger les données de SPC?
  - (5) regrouper et retourner les données au GC si la solution est abandonnée?
  - (6) signaler les incidents et les infractions touchant la sécurité?
- c) Quelles difficultés la conception et l'implantation de cette solution risquent-elles d'entraîner, et comment pourront-elles être surmontées? Quelles considérations propres au contexte gouvernemental faudra-t-il prendre en compte? Comment composeriez-vous avec des réseaux distincts qui ne communiquent pas entre eux (non classifiés, Protégés B, secrets)?
- d) IA et AA
- i) Comment entendez-vous élaborer des modèles conjuguant IA et AA pour éviter l'introduction de biais, potentiels ou non, et comment seraient-ils détectés?
  - ii) Comment l'industrie pourra-t-elle répondre à l'obligation de transparence des modèles d'IA-AA, essentielle à l'examen des prévisions de l'issue et à la compréhension des justifications (par exemple, quels facteurs ont le plus influencé l'issue prédite et de quelle manière a-t-elle évolué)? Dans ce contexte, quelles seraient les conséquences de la publication de l'information?
  - iii) Compte tenu des exigences formulées, quelles solutions éprouvées recommanderiez-vous à l'étape de la conception ou aux premiers stades de l'implantation? Existe-t-il des solutions qui satisfont à ces exigences, ou qui pourraient être personnalisées ou configurées en fonction de celles-ci? S'il n'existe pas de solution satisfaisant aux exigences, serait-il possible d'en concevoir une sur mesure en se fondant sur les technologies actuelles qui exploitent l'IA et l'AA? Veuillez expliquer.
  - iv) Est-il possible de mesurer la précision des prévisions de l'issue ou des tendances au moyen d'une marge d'erreur? Dans l'affirmative, quelle serait cette dernière?
  - v) Comment l'efficacité, la précision et la fiabilité d'une solution d'IA-AA pourraient-elles être assurées et mesurées? Veuillez faire des liens avec les capacités d'analyse et de prévision des solutions.
  - vi) Pouvez-vous établir des corrélations dans plusieurs domaines technologiques (calcul, réseau, nuage, stockage, etc.)?
  - vii) De quelle façon votre solution prend-elle en charge les périodes de maintenance et la gestion des changements? Peut-elle exploiter les données de l'outil de gestion des changements du système de GSTI (ServiceNow, Remedy ARS, SmartCloud d'IBM, etc.)?
  - viii) Votre solution peut-elle déterminer la cause fondamentale d'un incident en fonction d'incidents antérieurs? Contient-elle toute l'information ou doit-elle l'obtenir de notre outil de GSTI?
- e) L'efficacité, la précision, la fiabilité et la performance des solutions d'IA-AA pourraient-elles être évaluées en fonction de normes, de pratiques exemplaires ou de mesures de l'industrie?

- i) La surveillance étant un élément essentiel de la solution, expliquez comment son efficacité, sa précision et sa fiabilité seraient assurées et mesurées, surtout s'il s'agit d'une solution SaaS?
- ii) Veuillez fournir une matrice des responsabilités des intervenants ([RACI](#)) proposée par un fournisseur, ainsi que le point de vue de SPC.

Explication de l'acronyme RACI

R : responsable

A : agent comptable

C : consulté

I : informé

- f) Votre solution prend-elle en charge l'intégration fondée sur des services Web de transfert d'état représentationnel REST (Representational State Transfer) régis par des normes ouvertes?
- g) Pouvons-nous exporter des données sur les connaissances, de votre solution vers notre outil de GSTI?
- h) La technologie fonctionne-t-elle avec ou sans agent?
  - i) Quels en sont les avantages et les inconvénients?
- i) Veuillez donner un aperçu des services de formation et de soutien offerts, y compris en ce qui a trait à l'implantation de la solution à l'échelle du Canada et éventuellement dans divers ministères fédéraux et à l'étranger.
- j) Quel délai faut-il prévoir pour assurer la livraison d'une solution conforme aux exigences susmentionnées?
- k) Quelles sont les options possibles relativement aux droits de propriété intellectuelle, compte tenu des modèles d'affaires viables applicables aux solutions (propriété du fournisseur, propriété du GC, etc.)?
- l) Veuillez décrire les modèles de coûts possibles d'une solution appartenant au fournisseur (licence perpétuelle, par abonnement, licence d'utilisateur, d'appareil, d'unité centrale de traitement ou de serveur, d'organisme ou d'entreprise, etc.).
  - i) Quel serait un coût unitaire représentatif, calculé à partir de l'exemple d'inventaire fourni plus loin, en ce qui a trait à la surveillance des événements, à l'automatisation des dossiers d'exploitation et à l'IA dédiée aux opérations (AIOps)?
  - ii) Comment calculeriez-vous le coût unitaire de la solution APM? Ce coût doit être représentatif.
- m) Veuillez décrire en détail les différentes solutions APM capables d'assurer la surveillance d'applications maison et disponibles sur le marché.
- n) Veuillez décrire en détail la façon dont ces solutions pourraient s'intégrer à nos principaux outils.
- o) Veuillez fournir des exemples détaillés de la façon dont ces solutions peuvent enrichir les données sur les événements à partir de la BDGC et dont elles peuvent exploiter un outil de GSTI tiers à titre de système de consignation des incidents.
- p) Décrivez l'interface et le modèle d'authentification qui permet aux propriétaires d'infrastructure ou d'applications de mettre à jour les paramètres surveillés et les règles appliquées.

- q) SPC collige en ce moment les données relationnelles provenant de ses partenaires, de leurs applications opérationnelles et logiciels, ainsi que des instances de bases de données, de sites Web et de logiciels intermédiaires intégrées à leur infrastructure. Celle-ci comporte des éléments redondants, soit des interfaces se connectant à deux réseaux, un système de disques RAID (Redundant Array of Interdependent Disk), la réplication de site à site, des serveurs de base de données groupés ou des services ou dispositifs à charge équilibrée, etc. Comment votre technologie peut-elle aider SPC à comprendre pourquoi, à partir des données de la BDGC et de la topologie de réseau, une application du client ou d'entreprise risque de tomber ou l'est déjà, malgré les mécanismes de redondance présents dans l'environnement informatique?
- r) Au sujet du tableau de bord et du portail, veuillez indiquer la ou les solutions proposées et préciser si elles ont été évaluées en fonction des normes d'accessibilité EN 301 549, des règles pour l'accessibilité des contenus Web WCAG 2.0, WCAG 2.1 et WCAG 1.0, ainsi que des versions antérieure et postérieure à 2016 de l'article 508 du gouvernement américain.

### 3. Réponse des fournisseurs

#### 3.1 Présentation d'une réponse

- a) **Date et lieu de présentation des réponses?** Les fournisseurs qui souhaitent fournir une réponse doivent l'envoyer à l'autorité contractante par courriel à l'adresse électronique destinée à la présentation des réponses qui figure sur la page de couverture avant la date et l'heure limites indiquées sur la page de couverture du présent document.
- b) **Responsabilités en ce qui a trait à la présentation des réponses dans les délais prescrits :** Il incombe à chaque fournisseur de s'assurer que sa réponse est livrée à la bonne adresse électronique et qu'elle est reçue dans les délais prescrits.
- c) **Identification de la réponse :** Chaque fournisseur veillera à ce que son nom, l'adresse de l'expéditeur, le numéro de la demande d'information et la date de clôture apparaissent bien en vue dans la réponse. Le fournisseur doit également désigner un représentant avec lequel le gouvernement du Canada pourra communiquer au sujet de la réponse et indiquer le nom de la personne, son titre, son adresse, son numéro de téléphone et son adresse électronique.

#### 3.2 Confidentialité

Si un fournisseur juge que certaines parties de ses réponses sont exclusives ou confidentielles, celles-ci doivent porter clairement la mention exclusive ou confidentielle. Le gouvernement du Canada traitera les réponses conformément aux dispositions de la *Loi sur l'accès à l'information* et de toute autre loi en vigueur.

### 4. Examen des réponses par le gouvernement du Canada

#### 4.1 Examen des réponses

Les réponses ne feront pas l'objet d'une évaluation officielle. Toutefois, le gouvernement du Canada pourra utiliser les réponses reçues afin d'élaborer ou de modifier les ébauches de documents fournies avec la DDR ainsi que sa stratégie d'approvisionnement. Le gouvernement du Canada examinera l'ensemble des réponses reçues avant l'heure et la date de la clôture de la DDR. Il peut, à sa discrétion, les examiner après la date de clôture de la DDR.

#### 4.2 Équipe d'examen

Une équipe d'examen composée de représentants du gouvernement du Canada passera en revue et examinera les réponses. Le gouvernement du Canada peut faire appel à ses propres experts-conseils ou personnes-ressources pour examiner les réponses. Les membres de l'équipe d'examen ne participeront pas nécessairement tous à l'ensemble du processus d'examen.

### **4.3 Activité de suivi**

- a) Le gouvernement du Canada peut, à sa discrétion, communiquer avec tout fournisseur pour lui poser des questions supplémentaires ou demander des précisions concernant un aspect d'une réponse. Le suivi du gouvernement du Canada peut nécessiter une réponse écrite supplémentaire ou une réunion avec les représentants du gouvernement du Canada.