ANNEXE A

Solution de gestion des vulnérabilités d'entreprise
ÉNONCÉ DES TRAVAUX

1. INTRODUCTION

Services partagés Canada (SPC) est un ministère du gouvernement du Canada (GC) chargé de la transformation et de la gestion continue de l'infrastructure de TI des 43 ministères du GC. Cette spécification décrit les capacités des éléments d'infrastructure qui sont souhaitées pour soutenir le système de gestion des vulnérabilités de SPC. Les programmes et les données du gouvernement du Canada sont exposés à des risques inconnus en raison du manque de capacités de surveillance et de visibilité globales de SPC et de ses partenaires au sein de tous les environnements de TI. Cela nuit à la capacité de SPC d'avoir une vue d'ensemble des vulnérabilités existantes et d'être en mesure de prendre des mesures correctives. Le GC a besoin de services de gestion des vulnérabilités (SGV) d'entreprise efficaces, qui explorent et réduisent, de manière proactive et continue, les risques et les incidences résultant de l'exposition des systèmes, tout en étant un élément clé du cadre général de gestion des risques.

SPC a besoin de mettre en œuvre un système de gestion des vulnérabilités à l'échelle de l'organisation. Il s'agit d'un outil de prévention crucial utilisé quotidiennement par SPC pour détecter et confirmer les biens vulnérables au sein de notre infrastructure.

La portée du projet de SPC comprend l'acquisition, la configuration et le déploiement d'un ou de plusieurs outils de gestion des vulnérabilités d'entreprise dans les centres de données d'entreprise, les centres de données existants, l'infrastructure liée à Internet, et les points finaux du GC. La solution doit être capable d'effectuer la découverte des biens, les balayages des vulnérabilités, et les rapports des vulnérabilités pour un maximum de 2 000 000 de biens de TI. La portée du projet de SPC comprend également les communications et la collaboration entre les divers groupes, notamment : la gestion des vulnérabilités, la gestion des risques, la gestion des changements, la gestion des biens, la gestion des correctifs, les opérations de sécurité, les clients et les intervenants externes.

Ce projet exige aussi la conception d'une infrastructure de laboratoire permanente située dans la RCN, qui reproduit l'environnement de production. Ce laboratoire sera utilisé par SPC pour mettre à l'essai les configurations, les correctifs, les déploiements et les modèles de balayage avant qu'ils ne soient mis en œuvre dans les environnements de production. En plus, ce contrat exige la livraison d'une trousse de formation documentée propre au produit dispensée par un formateur du FEO certifié au personnel de SPC.

2. TERMINOLOGIE

Le tableau ci-dessous fournit des renseignements généraux sur les abréviations utilisées dans le présent énoncé des travaux (EDT).

GC	*Gouvernement du Canada*
SGV	*Système de gestion des vulnérabilités*
TI	*Technologie de l'information*
RCN	*Région de la capitale nationale*
FEO	*Fabricant d'équipement d'origine*
EDT	*Énoncé des travaux*
SPC	*Services partagés Canada*
RT	*Responsable technique*

3. RENSEIGNEMENTS GÉNÉRAUX

Le GC a reconnu la nécessité de déterminer et corriger les vulnérabilités des systèmes, car ces points faibles sont exploités par les auteurs de menaces. Le GC détient une myriade de systèmes et d'infrastructures de TI répartis à travers le monde, et les approches de gestion des vulnérabilités actuellement disparates ne sont ni réalistes ni durables du point de vue des offres de service d'entreprise.

Le projet de gestion des vulnérabilités d'entreprise de SPC permettra au GC de fournir des services aux environnements de TI d'entreprise par l'intermédiaire d'offres standard financées par SPC (p. ex., le balayage de centre de données d'entreprise, le balayage d'infrastructures de TI, le balayage de périmètre, le balayage de réseau, etc.); d'offres aux coûts recouvrés financées par les clients (p. ex., le balayage de poste de travail); et d'une approche itérative relative à un mécanisme d'approvisionnement à l'échelle du GC pour livrer des capacités de gestion des vulnérabilités financées et exploitées par les clients.

Dans de nombreux cas, les vulnérabilités de TI sont le résultat de défauts précédemment relevés ou connus, pour lesquels des correctifs ont déjà été publiés par la communauté des fournisseurs. Le SGV d'entreprise de SPC fournira une posture générale des risques en matière de sécurité renforcée grâce à la sensibilisation et à la visibilité globale sur les points faibles à l'échelle du GC. Cette connaissance contribuera à l'atténuation proactive des menaces à l'appui de la continuité des activités en général et de la protection des données.

4. OBJECTIFS

4.1. L'objectif principal du contrat est l'acquisition d'une solution de gestion des vulnérabilités d'entreprise destinée à remplacer l'infrastructure du SGV existante, ainsi qu'à augmenter nos capacités existantes. SPC développera la solution au fil du temps pour englober une plus grande partie de l'environnement du GC.

Les biens et les services suivants seront requis dans le cadre de cet effort :

- Le matériel et les logiciels nécessaires pour mettre en œuvre la solution, y compris :
    - Saisie et stockage des données
    - Création de rapports à partir des balayages
    - Réalisation d'analyse de sécurité complexe des données
    - Tenue à jour d'une base de données des biens
    - Réception des flux de données relatifs aux vulnérabilités
    - Réception des mises à jour de produits

4.2. Le deuxième objectif est la conception, la configuration et la mise à l'essai de l'environnement de laboratoire permanent satisfaisant aux exigences de SPC, qui servira d'environnement de préproduction pour mettre à l'essai les correctifs, les versions, les configurations et les modèles de balayage avant leur déploiement dans les environnements de production.

4.3. Le troisième objectif est de fournir un soutien technique à Services partagés Canada. Le soumissionnaire retenu doit fournir un point d'acheminement, que SPC peut utiliser pour demander un soutien en matière d'ingénierie et de soutien de la solution. En ce qui concerne le soutien technique, les services professionnels doivent être fournis par le FEO par téléphone ou en personne à court terme selon les besoins, et doivent être inclus dans le cadre du soutien et de la maintenance fournis par le soumissionnaire retenu.

4.4. Le quatrième objectif est la formation sur l'utilisation, le soutien et l'administration de la solution au sein du GC.

4.5. Le cinquième objectif est les services professionnels à court terme fournis par le fournisseur, qui seront utilisés dans le cadre de l'architecture, de la conception, de la construction et du déploiement du service. Les services professionnels fournis par le soumissionnaire doivent être habilités au niveau Secret du GC, et approuvés et certifiés par le FEO.

4.6. Les services professionnels doivent être inclus dans le prix de la soumission. Les services professionnels seront utilisés pendant une période d'au moins 60 (soixante) jours ouvrables afin d'aider à l'architecture de la solution.

4.7. Le soumissionnaire retenu sera invité à effectuer un essai d'acceptation pour démontrer que la solution présentée satisfait à un sous-ensemble d'exigences sélectionnées à partir des exigences obligatoires par SPC. Le soumissionnaire hébergera cet essai en utilisant ses propres installations, dispositifs et licences de produits. Le soumissionnaire doit démontrer clairement à SPC que sa solution peut répondre aux exigences à la satisfaction de SPC. Un pointage et des notes de passage seront attribués à chaque exigence. Les renseignements relatifs au pointage et à l'architecture proposée que SPC souhaite voir mise à l'essai seront inclus dans une annexe à la DP. SPC invitera d'autres soumissionnaires à participer à l'essai d'acceptation s'il s'avère que le soumissionnaire obtenant la note la plus élevée ne peut pas satisfaire aux exigences. Aspects obligatoires de l'essai d'acceptation :

- Le soumissionnaire doit fournir un accès physique à l'essai à 10 (dix) personnes de SPC.

- Le soumissionnaire n'a pas à se charger des frais de déplacement des personnes de SPC.

- Après l'invitation à participer à l'essai d'acceptation, le soumissionnaire disposera de 10 (dix) jours pour configurer son environnement de laboratoire en conformité avec l'architecture proposée par SPC.

- Le soumissionnaire dispose d'un maximum de cinq (5) jours pour démontrer à SPC qu'il répond à toutes les exigences d'essai.

- Les exigences obligatoires suivantes seront mises à l'essai. Les cas d'utilisation décrivant la façon dont SPC souhaite que l'essai soit réalisé sont fournis dans le plan d'essai d'acceptation inclus, qui sera présenté au soumissionnaire obtenant la note la plus élevée après la notation de la DP;

    - O1 – La solution doit soutenir pleinement la mise en œuvre, l'administration, la configuration et le balayage dans les réseaux IPv4 et IPv6
    - O2 – La solution doit être capable d'effectuer la découverte, l'inventaire et le suivi des biens, et les balayages des vulnérabilités pour 2 000 000 de biens de TI en réseau. Un balayage de découverte doit enregistrer 10 000 adresses IP en une seule journée. Un balayage complet de 10 000 adresses IP sans authentifiant doit être effectué sur une période de 2 jours, en l'étalant en dehors des heures de production de manière à réduire l'incidence sur les opérations quotidiennes. Un balayage complet de 10 000 adresses IP avec authentifiant doit être effectué sur une période de 3 jours, en l'étalant en dehors des heures de production de manière à réduire l'incidence sur les opérations quotidiennes.
    - O4 – La solution doit être capable de personnaliser le classement des risques par ordre de priorité en fonction du contexte opérationnel.
    - O6 – La solution doit avoir la capacité d'intégrer les résultats des balayages des vulnérabilités d'autres fournisseurs dans divers formats.

- O7 – La solution doit avoir la capacité de consommer et d'exécuter le contenu personnalisé ou du secteur conforme à SCAP 1.2 ou version ultérieure.
- O9 – La solution doit tenir à jour et stocker les journaux de vérification sécurisés conformément aux politiques du GC. (Voir http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12742)
- O11 – La solution doit être capable de traiter, de communiquer et de stocker les données en utilisant une méthode de chiffrement approuvée par le GC lorsque cela est jugé nécessaire (c.-à-d. sensibilité des données), utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques et des périodes cryptographiques qui ont été approuvés par le CST, validés par le Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), et sont spécifiés dans la norme ITSB-111 (https://www.cse-cst.gc.ca/fr/node/1428/html/25015) ou une version ultérieure;
- O13 – La doit identifier et authentifier les utilisateurs de l'organisation de manière unique par l'utilisation des services Active Directory de Microsoft.
- O18 – La solution doit avoir la capacité de sauvegarder tous ses éléments, ce qui inclut, mais ne s'y limite pas, la configuration des données de balayage.
- O27 – La solution doit fournir des capacités de découverte, regroupement, classification, et gestion des biens.

- SPC dispose d'un maximum de trois (3) jours pour examiner les résultats de l'essai d'acceptation.

- L'essai sera considéré comme un échec si le soumissionnaire obtenant la note la plus élevée ne satisfait pas aux exigences ou à la note de passage de l'essai d'acceptation. À ce stade, SPC choisira un autre soumissionnaire pour participer.

5. PORTÉE DES TRAVAUX

5.1. Le contrat de base comprend ce qui suit :

- Solutions de capacités d'entreprise et deux années de maintenance et de soutien. La solution peut être constituée de dispositifs réseau physiques, de serveurs virtuels ou de logiciels, pourvu qu'elle satisfasse à toutes les exigences obligatoires et aux critères cotés énoncés.

- La solution doit être capable d'effectuer des balayages de découverte des biens et des balayages des vulnérabilités pour 2 000 000 de dispositifs au minimum.

- La formation en salle de classe dirigée par un formateur (maximum de 10 élèves) organisée dans les bureaux de la RCN et peut-être les bureaux régionaux, d'une durée de 35 à 40 heures sur cinq (5) jours ouvrables consécutifs.

- Le soumissionnaire retenu doit fournir des services professionnels dans la période prévue dans la section Objectifs. Ces services professionnels seront utilisés pour aider à déployer la solution de manière efficace, y compris :

    - Ingénierie
    - Essais
    - Optimisation
    - Configuration du système
    - Création d'un environnement de laboratoire
    - Documentation sur le projet, au besoin

- Transfert des connaissances aux ressources de l'État

6. APERÇU DES PRODUITS LIVRABLES ET DU PAIEMENT

Produit livrable	**Critères évalués**	**Jours**
Acquisition d'une solution d'entreprise	Vérification d'attribution du contrat postérieure au plan d'essai.	5 jours
	Acceptation par SPC des résultats du plan d'essai	3 jours
Environnement de laboratoire permanent	Mise à l'essai/validation de la configuration du laboratoire du SGV	10 jours
	SPC reçoit tout le code source, les documents de conception et le document d'architecture relatifs à l'aménagement du laboratoire sous forme de copies imprimées et électroniques	
	Acceptation par SPC de la configuration du laboratoire du SGV	5 jours
Soutien technique	Fournir un point d'acheminement	
	Fournir des ressources de soutien ayant des connaissances approfondies sur le produit	
	Fournir des ressources de soutien dotées d'une expérience de la mise en œuvre et de l'architecture du produit à partir de zéro	
	Fournir des ressources de soutien dotées d'une expérience de déploiement d'entreprise de grande ampleur portant sur plus de 2 millions d'adresses IP	
Formation	Formation dispensée à un minimum de 10 ressources	
	Examen/validation par SPC de la formation sur le SGV	10 jours
	Acceptation par SPC de la formation dispensée	5 jours
Conception de l'architecture	Documentation sur la conception de l'architecture fournie par le fournisseur	
	Examen/validation de la conception de l'architecture du SGV	60 jours
	Acceptation par SPC de la conception de l'architecture du SGV	5 jours

7. PRODUITS LIVRABLES

7.1. Tous les produits livrables indiqués dans l'énoncé des travaux doivent être présentés au responsable technique (RT).

- L'ensemble du matériel et des logiciels inclus dans la solution de gestion des vulnérabilités d'entreprise, y compris l'ensemble des logiciels, des dispositifs, des adaptateurs de réseau et du stockage requis pour satisfaire à toutes les exigences obligatoires et à tous les critères cotés énoncés dans la soumission.

- L'abonnement pendant les 12 premiers mois aux flux portant sur les menaces relatives au produit doit être inclus.

7.2. Le produit livrable principal du contrat est l'acquisition d'une solution de gestion des vulnérabilités d'entreprise destinée à remplacer l'infrastructure de SGV existante, ainsi qu'à augmenter nos capacités existantes. SPC développera la solution au fil du temps pour englober une plus grande partie de l'environnement du GC.

Les biens et les services suivants seront requis dans le cadre de cet effort de remplacement :

- Le matériel et les logiciels nécessaires pour mettre en œuvre la solution, y compris :

  - Saisie et stockage des données
  - Création de rapports à partir des balayages
  - Réalisation d'analyse de sécurité complexe des données
  - Tenue à jour d'une base de données des biens
  - Réception des flux de données relatifs aux vulnérabilités
  - Réception des mises à jour de produits

7.3. La conception, la configuration et la mise à l'essai de l'environnement de laboratoire permanent satisfaisant aux exigences de SPC, qui servira d'environnement de préproduction pour mettre à l'essai les correctifs, les versions, les configurations et les modèles de balayage avant leur déploiement en production.

- Le matériel et les logiciels nécessaires pour mettre en œuvre la solution dans un environnement de laboratoire.

- Les services professionnels pour concevoir, configurer et installer l'environnement de laboratoire. Les services professionnels fournis par le soumissionnaire doivent être habilités au niveau Secret du GC, et approuvés et certifiés par le FEO.

- Les services professionnels pour effectuer la mise à l'essai de l'environnement de laboratoire terminé.

- Les services professionnels doivent fournir un rapport attestant que le laboratoire fonctionne selon les exigences convenues.

- Les services professionnels doivent fournir les documents de conception et tous les éléments connexes en version électronique et papier une fois que le laboratoire est terminé.

7.4. Soutien technique à Services partagés Canada

- Fournir un point d'acheminement, que SPC peut utiliser pour demander un soutien en matière d'ingénierie et de soutien de la solution. En ce qui concerne le soutien technique, les services professionnels doivent être fournis par le FEO par téléphone ou en personne à court terme selon les besoins, et doivent être inclus dans le cadre du soutien et de la maintenance fournis par le soumissionnaire retenu.

- Les services professionnels fournis par le soumissionnaire doivent être habilités au niveau Secret du GC, et approuvés et certifiés par le FEO.

- Fournir des ressources de soutien dotées de connaissances approfondies sur les suites de produit capables de traiter les demandes de soutien technique complexes.

- Fournir des ressources de soutien dotées d'une expérience de la mise en œuvre et de l'architecture du produit à partir de zéro jusqu'à l'état final.

- Fournir des ressources de soutien dotées d'expérience de grands déploiements portant sur des infrastructures de plus d'un million d'adresses IP.

- Le soutien doit être disponible dans les deux langues officielles.

- Le soutien doit être disponible 24 heures sur 24.

7.5. Cinq (5) jours consécutifs de formation en salle de classe (10 élèves maximum) sur l'utilisation, le soutien et l'administration de la solution. Les services professionnels relatifs à la formation doivent être inclus dans le prix de la soumission.

7.6. Les services professionnels seront utilisés pendant une période d'au moins 60 (soixante) jours ouvrables afin d'aider à l'architecture de la solution.

- Services professionnels à court terme fournis par le fournisseur dotés d'une habilitation de sécurité au niveau Secret du GC afin de concevoir, construire et déployer la solution. Les services professionnels doivent être certifiés par le FEO des produits présentés.

- Les services professionnels créeront l'architecture et la conception du SGV.

- Les services professionnels fourniront toute l'architecture, l'architecture de la solution, la conception détaillée, les livrets de conception, les renseignements relatifs au soutien, et les documents de conception sous forme de copies électroniques et imprimées.

- Les services professionnels fourniront le code personnalisé de cette solution, y compris, les commentaires du code; les scripts personnalisés doivent être fournis à SPC en format brut.

- Transfert des connaissances aux ressources désignées de l'État, au besoin.

- Les services professionnels fourniront tous les documents qui ont été créés lors de la construction sous forme imprimée et électronique à SPC.

- Les services professionnels répondront à toutes les préoccupations ou questions qui n'ont pas été abordées jusque-là.

- Les services professionnels veilleront à ce que le RT et les ressources de l'État aient une compréhension détaillée de la solution et de l'infrastructure de soutien.

- Les services professionnels fourniront un document récapitulant toutes les questions et préoccupations qui ont été soulevées lors de la construction et de l'architecture.

7.7. Le volet optionnel du contrat comprend ce qui suit :

- L'option d'acheter les services de maintenance et de soutien pour les années d'option (années 3, 4 et 5) de l'équipement acheté dans le cadre de l'exigence du contrat de base.

- L'option d'acheter des solutions matérielles de capacités d'entreprise supplémentaires pour l'expansion au-delà de l'exigence initiale de 2 000 000 de dispositifs. L'option d'acheter une année de soutien supplémentaire pendant au plus trois (3) ans au prix initial de la soumission. L'option d'acheter des trousses de formation de cinq (5) jours supplémentaires pendant au plus trois (3) ans au prix établi dans la soumission.

8. BIENS LIÉS AUX SERVICES PROFESSIONNELS RENDUS SUR PLACE

8.1. Les ressources doivent être en mesure de travailler dans les locaux du gouvernement du Canada situés dans la région de la capitale nationale (RCN). Des postes de travail informatisés seront fournis.

Les déplacements dans la RCN seront fréquents. Les frais de déplacement dans la RCN ne seront pas remboursés.

8.2. Les ressources qui fournissent des services professionnels travailleront sous la supervision d'un responsable technique ou d'un gestionnaire.

8.3. Le fournisseur doit joindre des rapports d'étape à toutes ses factures.

8.4. Des ressources de bureau seront fournies aux ressources.

8.5. Si les données considérées comme des informations privées sont traitées, l'entrepreneur doit présenter au Canada un guide de gestion des services pour la solution de gestion de la vulnérabilité de l'entreprise à Services partagés Canada (SPC) qui comprend :

8.6. Si les données considérées comme des informations privées sont traitées , l'entrepreneur doit envoyer au responsable technique un rapport sur les atteintes à la vie privée, qui couvre la période de référence précisée par le Canada et qui contient :

a) le nombre d'incidents d'atteinte à la vie privée;

b) le nombre d'enquêtes réalisées sur des atteintes à la vie privée;

c) les délais d'intervention moyen et maximal pour les incidents d'atteinte à la vie privée..

8.7. Les ressources qui fournissent des services professionnels doivent détenir une habilitation de sécurité canadienne valide de niveau Secret. Le soumissionnaire doit préciser le numéro de dossier de l'habilitation de sécurité et sa date d'échéance.

8.8. Les ressources travailleront pendant les heures normales de travail, soit pas avant 7 h et pas plus tard que 18 h, heure locale, du lundi au vendredi. Les ressources doivent travailler 7,5 heures par jour pendant l'horaire de travail habituel, sauf si d'autres ententes sont prévues avec le responsable technique.

8.9. Les ressources doivent être capables de communiquer efficacement en anglais, tant à l'oral qu'à l'écrit.

8.10. Les ressources doivent fournir la gestion de projet relative aux regroupements, conversions et transformations de TI en cours.

8.11. Les ressources doivent fournir l'administration des systèmes pour tout système ou application de sécurité des TI, selon les besoins.

8.12. Les ressources doivent fournir un soutien opérationnel pour tout système ou application de sécurité des TI, selon les besoins.

8.13. Les ressources doivent effectuer les mises à niveau logicielles et apporter les correctifs.

8.14. Les ressources doivent installer des équipements neufs ou de rechange, selon les besoins.

8.15. Les ressources doivent créer ou tenir à jour une base de données des équipements contenant les numéros de série et les contrats de maintenance des équipements, selon les besoins.

8.16. Les ressources doivent mettre à l'essai les flux de travail avec les partenaires et les groupes de pairs, selon les besoins.

8.17. Les ressources doivent conserver, créer et mettre à jour les documents de construction et la documentation opérationnelle selon les exigences de la charge de travail.

9. BIENS LIÉS AUX SERVICES DE FORMATION

9.1. Les ressources dispensant la formation doivent être disponibles pour travailler dans les installations du GC principalement au sein de la région de la capitale nationale; mais la formation peut également être nécessaire en dehors de la RCN.

9.2. Les ressources dispensant la formation travailleront sous la supervision d'un responsable technique ou d'un gestionnaire.

9.3. Les ressources recevront des ressources de bureau, mais devront fournir les ordinateurs.

9.4. Les ressources doivent être dotées d'une habilitation de sécurité de niveau Fiabilité du gouvernement du Canada.

9.5. Les ressources travailleront pendant les heures normales de travail, soit pas avant 7 h et pas plus tard que 18 h, heure locale, du lundi au vendredi.

9.6. Les ressources doivent être capables de communiquer efficacement en anglais, tant à l'oral qu'à l'écrit. Le bilinguisme (anglais et français) est souhaitable, mais pas obligatoire.

10. RENSEIGNEMENTS EXCLUSIFS

10.1. Non-divulgation

- Tous les travaux exécutés par l'entrepreneur dans le cadre du présent énoncé des travaux demeureront la propriété de l'État. Les rapports, documents et prolongations afférentes demeurent la propriété de l'État, et l'entrepreneur ne pourra divulguer ou diffuser de tels rapports ou documents à une autre personne, ni les reproduire, sans l'autorisation écrite préalable de l'État.

- Tous les renseignements et les documents mis à la disposition de l'entrepreneur dans le cadre du présent projet sont jugés exclusifs et doivent être restitués à l'État une fois les tâches décrites dans le présent énoncé des travaux réalisés ou à la résiliation du contrat.

N.B: Les articles 11 à 14 inclusivement ne s'appliquent que si l'entrepreneur et/ou le vendeur traitent des renseignements personnels. Ces clauses peuvent être ignorées si le fournisseur ne traite pas d'informations personnelles.

11. PLAN DE GESTION DE LA CONFIDENTIALITÉ

11.1. Dans son plan de gestion des renseignements personnels, l'entrepreneur démontre qu'il est en mesure de satisfaire aux exigences du contrat et de fournir l'assurance de sa capacité à gérer les dossiers et les renseignements personnels conformément aux obligations imposées par la loi.

11.2. L'entrepreneur doit soumettre une ébauche du plan de gestion des renseignements personnels dans les 60 jours ouvrables du gouvernement fédéral suivant l'attribution du contrat par le Canada aux fins d'approbation. Le Canada se réserve le droit de demander qu'on apporte des modifications au plan afin de s'assurer que les renseignements personnels sont adéquatement gérés par l'entrepreneur.

11.3. A la demande du Canada, l'entrepreneur doit présenter une version actualisée de son plan de gestion des renseignements personnels dans les 20 jours ouvrables du gouvernement fédéral suivant la demande.

11.4. Le plan de gestion des renseignements personnels doit décrire expressément les éléments suivants en détail :

- les stratégies de protection des renseignements personnels de l'entrepreneur et la description détaillée du traitement exact des renseignements personnels tout au long de leur cycle de vie;

- les méthodes employées pour recueillir, utiliser, conserver et divulguer les renseignements personnels exclusivement aux fins d'exécution des travaux prévus au contrat;

- les méthodes employées pour restreindre l'accès aux renseignements personnels et aux dossiers aux personnes autorisées seulement (selon le principe du besoin de connaître) et exclusivement aux fins d'exécution des travaux prévus au contrat;

- le protocole à suivre en cas d'atteinte à la vie privée et les méthodes employées pour traiter une telle situation;

- les méthodes que l'entrepreneur entend employer pour veiller à ce que les exigences en matière de protection des renseignements personnels du Canada décrites dans la Loi sur la protection des renseignements personnels, la Loi sur l'accès à l'information et la Loi sur la Bibliothèque et les Archives du Canada soient respectées tout au long de l'exécution des travaux et pendant toute la durée du contrat;

- toute nouvelle mesure que l'entrepreneur entend mettre en œuvre pour protéger les renseignements personnels et les dossiers en fonction de leur classification de sécurité;

- les méthodes que l'entrepreneur entend employer pour veiller à ce que les rapports renfermant des renseignements personnels soient stockés ou transmis de façon sécuritaire en fonction de leur classification de sécurité;

- décrire la manière dont l'entrepreneur compte veiller à ce que son personnel soit formé sur la protection des renseignements personnels et les principes liés à ceux-ci.

12. ÉVALUATION DES FACTURES RELATIFS À LA VIE PRIVÉE

12.1. L'entrepreneur doit aider le Canada à réaliser l'évaluation des facteurs relatifs à la vie privée (EFVP) conformément à la Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308&section=text#cha1). À cette fin, il doit fournir les renseignements suivants dans les 20 jours ouvrables du gouvernement fédéral suivant une demande de SPC à cet égard :

- les processus opérationnels, les flux de données et les procédures de collecte, de transmission, de traitement, de stockage, d'élimination et de consultation des renseignements, y compris des renseignements personnels;

- la liste des renseignements personnels utilisés par l'entrepreneur dans le cadre des travaux et le but de chaque élément de renseignements personnels;

- les modes de transmission des renseignements personnels et les destinataires des renseignements;

- la liste de tous les emplacements où les exemplaires papier des renseignements personnels sont conservés;

- la liste de tous les emplacements où les renseignements personnels sous forme lisible par machine sont conservés (p. ex., emplacement du serveur sur lequel la base de données est installée), ainsi que les sauvegardes de sécurité;

- la liste de toutes les mesures prises par l'entrepreneur pour protéger les renseignements personnels et les dossiers outre celles qui sont exigées en vertu du contrat;

- les exigences ou recommandations relatives à la sécurité et à la protection des renseignements personnels à suivre;

- une explication détaillée des menaces réelles ou potentielles touchant les renseignements personnels ou les dossiers, accompagnée d'une évaluation des risques liés à ces menaces et de la pertinence des protections existantes visant à les prévenir;

- les résultats des consultations (le cas échéant) découlant d'un examen de l'évaluation des facteurs relatifs à la vie privée par le Commissariat à la protection de la vie privée du Canada (CPVP) et approuvés par ce dernier.

12.2. L'entrepreneur doit prêter son concours au Canada pendant la préparation de l'évaluation des facteurs relatifs à la vie privée et appliquer les recommandations qui en découlent en fonction d'un échéancier approuvé par le Canada, sans frais pour le Canada.

12.3. Si des changements prévus à la solution de gestion de la vulnérabilité de l'entreprise ont une incidence sur l'utilisation, la collecte, le traitement, la transmission, le stockage ou l'élimination de renseignements personnels, ou lorsque SPC en fait la demande, l'entrepreneur doit transmettre à ce dernier de l'information suffisamment détaillée pour justifier une mise à jour de l'évaluation des facteurs relatifs à la vie privée et lui faire approuver les changements prévus.

12.4. L'entrepreneur doit remettre un dossier de sensibilisation à la protection des renseignements personnels à son personnel impliqué dans les services de centres d'appels hébergés de SPC. Le dossier doit donner un aperçu de l'utilisation des renseignements personnels.

13. MISE EN ŒUVRE DU PLAN DE GESTION DES RENSEIGNEMENTS PERSONNELS

13.1. L'entrepreneur doit mettre en œuvre le plan de gestion des renseignements personnels (processus, procédures, rôles, responsabilités, etc.) et appliquer toute mise à jour subséquente annuelle dans les 60 jours ouvrables du gouvernement fédéral suivant l'acceptation des services par SPC.Afadfdafadsfdas

13.2. L'entrepreneur doit présenter à SPC, dans les 40 jours ouvrables du gouvernement fédéral suivant une demande à cet égard, la preuve, qui peut prendre la forme de résultats d'essais, d'évaluations, de vérifications ou autres, et ne peut dater de plus de 12 mois, que le plan de gestion des renseignements personnels a été convenablement mis en œuvre, qu'il fonctionne comme prévu, qu'il produit les résultats escomptés et qu'il satisfait aux exigences du Canada en matière de protection des renseignements personnels.

13.3. Si l'entrepreneur détermine qu'il lui faudra plus de 40 jours ouvrables du gouvernement fédéral pour présenter la preuve demandée, il doit en aviser SPC au plus tard 5 jours ouvrables du gouvernement fédéral suivant la demande de preuve initiale et solliciter par écrit une prolongation en fournissant la justification appropriée. La décision d'accorder ou non une prolongation sera laissée à la discrétion de SPC.

13.4. S'il prévoit des changements aux services de centres d'appels hébergés de SPC touchant l'utilisation, la collecte, le traitement, la transmission, le stockage ou l'élimination de renseignements personnels, ou si SPC lui en fait la demande, l'entrepreneur doit présenter à ce dernier de l'information suffisamment détaillée pour justifier la mise à jour de

l'évaluation des facteurs relatifs à la vie privée et lui faire approuver les changements prévus.

13.5. Dans les 40 jours ouvrables du gouvernement fédéral suivant l'attribution du contrat, l'entrepreneur accepte de fournir une trousse de formation et sensibilisation d'une page pour informer ses employés et ses consultants de l'utilisation des renseignements personnels fournis par le Canada au sujet des utilisateurs.

14. ENQUÊTES LES PLAINTES ET DEMANDES D'ACCÈS À L'INFORMATION

14.1. Pendant toute la durée du contrat, l'entrepreneur doit exécuter les processus et les contrôles visant à assurer l'intégrité, la confidentialité et l'exactitude de l'ensemble des données et des métadonnées, peu importe leur format, qui sont en sa possession ou sous sa garde et qui ont été générés ou acquis dans le cadre du contrat, ou encore qui sont liées de quelque autre façon à ses responsabilités et à ses obligations stipulées au contrat, pour s'assurer qu'elles puissent être présentées comme preuve convaincante à un tribunal.

14.2. L'entrepreneur doit, dans la mesure permise par la loi, offrir son entière collaboration au Canada, entre autres en l'aidant à mener des enquêtes sur les plaintes, des enquêtes réglementaires ou judiciaires et des poursuites en matière réglementaire ou judiciaire et en répondant aux demandes d'accès à l'information, y compris en permettant des inspections et des vérifications de sécurité et en fournissant les renseignements voulus (documentation, description des modes de protection des données, architecture de données et descriptions relatives à la sécurité) dans les 5 jours ouvrables du gouvernement fédéral suivant une demande du Canada à cet égard.

15. INTERPRÉTATION

15.1. En cas de différends dans l'interprétation du présent énoncé des travaux ou de la terminologie qu'il contient, la décision du responsable technique a préséance.