Service de sécurité géré du gouvernement du Canada (SSGGC)

Annexe A : Énoncé des travaux

Date : 12 juillet 2012

TABLE DES MATIÈRES

INDEX DES TABLEAUX

1 INTRODUCTION

(1) Le gouvernement du Canada (désigné ci-après « le Canada ») a besoin d'un service de sécurité géré du gouvernement du Canada (SSGGC).

2 PRÉPARATION OPÉRATIONNELLE

2.1 Lancement du contrat

(2) Le Canada organisera une réunion pour le lancement du contrat; cette réunion se tiendra dans les 10 jours civils suivant l'adjudication du contrat.

(3) Le représentant de la haute direction de l'entrepreneur devrait agir comme dirigeant responsable du contrat, et celui-ci devrait assister à la réunion visant le lancement du contrat.

(4) L'ordre du jour de la réunion sera établi par le Canada et transmis à l'entrepreneur au moins trois jours ouvrables de la fonction publique fédérale (JOFPF) avant celle-ci.

2.2 État de préparation du projet

(5) L'entrepreneur doit, dans les 10 jours civils suivant l'adjudication du contrat, soumettre un plan de gestion de projet (PGP) provisoire pour approbation par le Canada. Dans le PGP, l'entrepreneur indique comment il gérera le projet. Le PGP doit traiter des sujets qui suivent, selon le *Guide PMBOK*® (4e édition) :

a) Le plan de gestion des exigences;

b) Le plan des ressources humaines, notamment :

i) L'organigramme;

ii) Les rôles et responsabilités;

iii) La gestion des conflits et les paliers d'intervention;

c) Le plan de gestion des communications;

d) Le plan de gestion des risques du projet;

e) Le plan de gestion de la qualité;

f) Le plan de gestion des changements.

(6) L'entrepreneur doit fournir un PGP définitif dans les cinq jours civils suivant la réception des commentaires du Canada concernant le PGP provisoire.

(7) L'entrepreneur doit, dans les 15 jours civils suivant l'adjudication du contrat, présenter une méthode de mise en œuvre du service (MMS) provisoire pour approbation par le Canada. Cette méthode décrit la méthodologie qu'il compte appliquer pour être prêt sur le plan opérationnel et traite des éléments qui suivent :

a) L'aperçu des phases de mise en œuvre et des points de contrôle;

b) La séquence des phases et des activités;

c) Les dépendances entre les activités des différentes phases;

d) Les critères de fin de phase;

e) Les critères de fin d'activité;

f) Les critères à la fin du point de contrôle;

g) Les jalons;

h) Les produits/livrables par activité;

i) L'aperçu des produits/livrables;

j) L'intégration dans la méthodologie des livrables et des activités connexes du contrat;

k) L'intervention requise du Canada au niveau de l'activité, accompagnée d'une description des compétences recherchées.

(8) L'entrepreneur doit présenter une MMS définitive dans les cinq jours civils suivant la réception des commentaires du Canada concernant la MMS provisoire.

2.3 Plan de préparation opérationnelle

(9) L'entrepreneur doit, dans les 39 jours civils suivant l'adjudication du contrat, soumettre, pour approbation par le Canada, un plan de préparation opérationnelle (PPO) provisoire fondé sur la MMS définitive et précisant ce qui suit :

a) Un échéancier, en format Microsoft Project 2003, au terme duquel il prévoit être prêt sur le plan opérationnel, suivant l'adjudication du contrat, qui précise ce qui suit :

i) La liste des phases, points de contrôle, livrables et jalons de la MMS, sous forme de tâches distinctes;

ii) La date de début et de fin de chaque tâche;

iii) La durée de chaque tâche;

iv) L'attribution de chaque tâche de faible niveau à un groupe de ressources;

v) La détermination, selon la MMS, des dépendances de chaque tâche;

vi) L'incidence des dépendances, de la durée et des ressources sur les dates de début et de fin de chaque tâche;

vii) La désignation de chaque livrable du projet comme jalon;

viii) La limitation autant que possible des dépendances entre les tâches;

ix) Dans toute la mesure du possible, l'exécution des tâches en parallèle;

x) La remise progressive des livrables au Canada;

xi) L'échéancier n'impose pas de recours inutile à l'examen et à l'approbation du Canada;

xii) La détermination, dans l'échéancier, du moment auquel il est nécessaire de recourir à l'examen et à l'approbation du Canada;

xiii) La détermination, dans l'échéancier, du type de ressource du Canada nécessaire pour fournir des commentaires à l'entrepreneur, ainsi que du moment auquel ces ressources sont requises et la période pendant laquelle elles le sont;

xiv) La conformité de l'échéancier avec les obligations contractuelles de produire certains livrables après un nombre de jours déterminé;

b) Une liste des hypothèses formulées pour le PPO;

c) Une évaluation du risque, en conformité avec le plan de gestion des risques du projet, comportant les caractéristiques suivantes :

i) La détermination de l'ensemble des risques du projet;

ii) Le classement de chaque risque;

iii) La probabilité rattachée à chaque risque;

iv) Les répercussions susceptibles de se produire si le risque se concrétise;

v) Les mesures d'atténuation;

vi) Les mesures de surveillance;

vii) L'attribution du risque.

(10) L'entrepreneur doit fournir un PPO définitif dans les cinq jours civils suivant la réception des commentaires du Canada concernant le PPO provisoire.

2.4 Travaux visant la préparation opérationnelle

(11) À moins d'indication contraire, l'entrepreneur doit fournir les produits livrables qui suivent dans les 120 jours civils suivant l'acceptation du PPO et respecter l'échéancier figurant dans le PPO approuvé. Sont exclus de la période de 120 jours civils, les jours dont a besoin le Canada pour examiner et approuver les travaux accomplis, notamment :

a) Le pPlan de gestion du service (voir la sous-section Plan de gestion du service);

b) Le pPlan de continuité du service (voir la sous-section Plan de continuité du service);

c) Le pPlan de transition du service (voir la sous-section Plan de transition du service);

d) La cConception du service (voir la sous-section Conception du service);

e) La

matrice de traçabilité des exigences fonctionnelles (voir la sous-section

Matrice de traçabilité des exigences fonctionnelles);

f) La description du service (voir la sous-section Description du service);

g) La certification et accréditation en matière de sécurité (voir la sous-section Certification et accréditation en matière de sécurité);

i) le concept de sécurité des opérations (voir la sous-section Concept de sécurité des opérations);

ii) le plan de gestion du risque de sécurité (voir la sous-section Plan de gestion du risque de sécurité);

iii) l'architecture de sécurité (voir la sous-section Architecture de sécurité);

iv) les procédures d'exploitation de la sécurité (voir la sous-section Procédures d'exploitation de la sécurité);

v) la matrice de traçabilité des exigences de sécurité (voir la sous-section Matrice de traçabilité des exigences de sécurité);

vi) la vérification de la sécurité (voir la sous-section Vérification de la sécurité);

vii) la test de sécurité (voir la sous-section Test de sécurité);

viii) l'évaluation et atténuation des vulnérabilités (voir la sous-section Évaluation et atténuation des vulnérabilités);

ix) Le plan de traitement des risques (voir la sous-section Plan de traitement des risques);

h) La mise en œuvre du SSGGC (voir la sous-section Mise en œuvre du SSGGC).

(12) L'entrepreneur doit appliquer la MMS approuvée et respecter l'échéancier figurant dans le PPO approuvé, pour gérer le projet.

(13) L'entrepreneur doit fournir au Canada un rapport d'étape hebdomadaire portant sur la préparation opérationnelle, dans lequel il indiquera, pour chaque tâche, jalon ou produit livrable figurant dans le PPO, les renseignements qui suivent :

a) La situation actuelle;

b) La date prévue d'achèvement;

c) Les problèmes et les mesures d'atténuation proposées;

d) Les risques et les mesures d'atténuation proposées;

e) Le résumé des activités de travail prévues pour la prochaine semaine visée par le rapport.

2.5 Plan de gestion du service

(14) L'entrepreneur doit fournir au Canada un plan de gestion du service qui comprend ce qui suit :

a) Une description sommaire du SSGGC;

b) Un plan des ressources décrivant la méthodologie élaborée pour déterminer les ressources nécessaires pour l'exécution des travaux prévus au contrat et évaluer les compétences et les aptitudes de celles-ci à s'acquitter des fonctions exigées;

c) Un plan d'assurance de la qualité décrivant l'approche retenue pour concevoir et appliquer les normes quantitatives et qualitatives, assurer la conformité aux niveaux de service et examiner le travail en cours;

d) Un plan de communication décrivant l'approche envisagée pour communiquer les exigences inhérentes à chaque tâche, résoudre les problèmes (techniques et ceux liés au service et au personnel) et les risques qui touchent l'entrepreneur et le Canada, et gérer les communications entre ces parties;

e) Un plan organisationnel précisant la structure de gestion, les organisations, et les rôles et responsabilités liés au personnel clé et aux experts en la matière;

f) Un plan de gestion des risques décrivant l'approche envisagée pour cerner les risques et en faire le suivi, repérer les déclencheurs d'événements liés aux risques, évaluer les probabilités et les incidences et concevoir un plan d'atténuation;

g) Un plan de gestion des problèmes exposant l'approche retenue pour cerner et gérer les problèmes liés à la gestion du service, isoler les problèmes, en évaluer l'incidence et le niveau de gravité, identifier les parties responsables et analyser les priorités et processus en vue de déterminer une solution;

h) Un aperçu décrivant les systèmes d'information qui seront mis en œuvre pour le SSGGC.

2.6 Plan de continuité du service

(15) L'entrepreneur doit fournir au Canada un plan de continuité du service qui prévoit, aux fins de reprise des activités du SSGGC après sinistre, ce qui suit :

a) Une stratégie pour le rétablissement du service;

b) Une analyse des répercussions d'une interruption de service sur les activités;

c) Les processus qui seront appliqués pour assurer la continuité du service (par exemple la stratégie de communication, l'établissement des priorités à l'égard du rétablissement du service);

d) Son plan visant le transfert des fonctionnalités opérationnelles et de gestion du centre principal des opérations au centre des opérations de secours;

e) Les stratégies de secours s'appliquant aux installations, données et systèmes de soutien opérationnel, et composantes clés du service;

f) La façon dont il s'assurera que ses fournisseurs (le cas échéant) ont mis en place des stratégies et des plans de reprise après sinistre;

g) La façon dont il remplacera les fournisseurs clés au besoin;

h) La démarche qu'il suivra pour démontrer que son plan est efficace et que ses opérations sont en mesure de réagir en cas de sinistre.

2.7 Plan de transition du service

(16) L'entrepreneur doit fournir au Canada un plan de transition du service qui décrit la manière dont les organisations clientes effectueront la transition des Services de sécurité gérés (SSG) existants au nouveau SSGCC. Le plan de transition comprend ce qui suit :

a) Une description détaillée du processus de transition;

b) Un plan de projet indiquant les jalons, les dépendances, la date prévue du commencement de la transition, ainsi que la date d'achèvement de celle-ci;

c) Les risques associés au processus de transition proposé, ainsi que les mesures d'atténuation ou d'urgence proposées lorsque les risques peuvent avoir une incidence sur le service;

d) L'impact prévu sur la sécurité, la performance, l'expérience utilisateur, la prestation des services et la capacité de reprise;

e) Les procédures de retour arrière;

f) Un plan de test visant à s'assurer que la transition s'est effectuée avec succès.

(17) Le processus de transition du service doit veiller à ce que les règles, politiques, signatures de menaces et toute autre configuration courantes des SSG existants soient répertoriés, examinés, optimisés et mis en œuvre dans le SSGGC.

(18) Le processus de transition du service ne doit pas affaiblir la protection contre les menaces que fournissent les SSG existants aux organisations clientes.

2.8 Conception du service

(19) L'entrepreneur doit fournir au Canada, à l'égard du SSGGC, une conception du service qui prévoit ce qui suit :

a) La méthodologie de conception;

b) Un plan détaillé de l'architecture de la solution;

c) Les éléments d'architecture qui décrivent les composantes du produit et du service, notamment en ce qui concerne les interfaces;

d) Une architecture de déploiement qui décrit l'affectation de composantes de service logiques aux nœuds informatiques virtuels et (ou) physiques et met en évidence les caractéristiques de redondance, d'extensibilité et de sécurité de l'architecture qui appuient les niveaux de service;

e) Une architecture de sécurité réseau qui décrit la mise en œuvre de mesures de protection du périmètre de sécurité, l'affectation des services dans les zones de sécurité du réseau et les caractéristiques de redondance, d'extensibilité et de sécurité de l'architecture qui appuient les niveaux de service;

f) Un graphique de réseau qui comprend les topologies physique et logique du réseau, de façon à représenter les nœuds et les connexions, les protocoles réseau, les sous-réseaux d'adresses de protocole Internet (IP) et la bande passante du réseau;

g) Le contenu et le format des rapports et des documents;

h) Une conception du portail de services comprenant ce qui suit :

   i) Les spécifications fonctionnelles;

   ii) Une maquette des pages du portail de services;

   iii) Une description du cheminement des pages du portail de services;

i) Le nom des fabricants de l'équipement qu'il installera sur le réseau du Canada aux fins du SSGGC;

j) Le nom des fabricants de l'équipement qu'il a installé ou qu'il installera sur sa propre infrastructure réseau ou sur celle d'un tiers et qui sera interconnecté avec le réseau du Canada aux fins du SSGGC;

k) L'intégration avec les services ne faisant pas partie des domaines du SSGGC;

l) La démarche de migration envisagée à partir des services existants précisés par le Canada;

m) Les besoins matériels et les exigences de préparation du site (p. ex. source d'énergie, locaux, enjeu environnemental) s'appliquant aux services gérés du SSGGC au point de prestation de services (PPS) du Canada.

(20) La conception du service s'appliquant au SSGGC doit veiller à ce que les composantes matérielles et logicielles du SSGGC déployées au PPS du Canada soient dédiées au Canada.

2.9 Matrice de traçabilité des exigences fonctionnelles

(21) L'entrepreneur doit fournir au Canada une matrice de traçabilité des exigences fonctionnelles (MTEF), ainsi que les documents connexes portant sur le service, qui offre des renvois à l'information décrivant de quelle façon chaque composante des applications répond à chacune des exigences fonctionnelles indiquées dans l'Énoncé des travaux.

(22) Les documents mentionnés dans la MTEF doivent décrire la composante de l'application de façon suffisamment détaillée pour permettre au Canada de confirmer qu'elle satisfait aux exigences fonctionnelles figurant dans l'Énoncé des travaux.

2.10 Description du service

(23) L'entrepreneur doit fournir au Canada, à l'égard du SSGGC, une description du service comprenant de l'information sur ce qui suit :

a) L'aperçu du SSGGC;

b) Les procédures de mesure des niveaux de service;

c) L'aperçu des rapports sur le service;

d) Les processus des services de gestion (gestion des changements, des incidents, de la configuration, des mises en production, de la disponibilité et de la capacité);

e) Les procédures concernant le centre de services;

f) Les procédures concernant le centre des opérations;

g) Les procédures concernant le centre des opérations de sécurité de l'information.

2.11 Certification et accréditation en matière de sécurité

(24) L'entrepreneur doit exécuter les travaux figurant dans la présente sous-section, dans le cadre du processus de certification et d'accréditation en matière de sécurité du Canada pour le SSGGC, à l'égard de chaque service de gestion des menaces du SSGGC, du service de gestion des informations et des événements de sécurité (GIES) et de chaque variante de la solution s'y rapportant.

2.11.1 Concept de sécurité des opérations

(25) L'entrepreneur doit fournir au Canada un rapport concernant le concept de sécurité des opérations qui décrit ce qui suit :

a) Les utilisateurs;

b) Ses applications servant à l'exploitation du service;

c) Ses installations des centres de données;

d) Ses responsabilités et rôles en matière de sécurité, et ceux du Canada;

e) Les contrôles d'accès;

f) L'environnement opérationnel qu'il exploite.

2.11.2 Plan de gestion du risque de sécurité

(26) L'entrepreneur doit fournir au Canada un plan de gestion du risque de sécurité qui indique :

a) La manière dont les risques de sécurité seront signalés (à qui et à quelle fréquence);

b) Les rôles et responsabilités à l'égard de la gestion du risque de sécurité;

c) La manière dont les risques de sécurité seront suivis et traités.

2.11.3 Architecture de sécurité

(27) L'entrepreneur doit fournir au Canada un rapport portant sur l'architecture de sécurité qui indique ce qui suit à l'égard de son infrastructure pour les opérations, l'administration et la gestion :

a) La façon dont les interfaces aux zones d'accès public (les publications ITSG-22 [http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-fra.pdf] et ITSG-38 [http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg38-fra.pdf] du Centre de la sécurité des télécommunications Canada (CSTC) décrivent ce que sont les zones d'accès public) sont rigoureusement contrôlées, y compris tous les réseaux externes, tels qu'Internet, selon un périmètre de sécurité défini;

b) Comment les autres zones de sécurité du réseau sont établies conformément à la publication ITSG-22 du CSTC;

c) La façon dont un système réseau de détection des intrusions est établi dans chaque zone de sécurité et dont un système de détection des intrusions sur hôte est établi sur les principaux hôtes;

d) Comment les mécanismes de défense du périmètre (p. ex. pare-feu, routeurs, passerelles d'applications) sont mis en place pour gérer le trafic de données et protéger les serveurs accessibles à partir d'Internet;

e) Les composantes de système utilisant des produits ayant reçu une certification d'évaluation du niveau d'assurance en vertu des critères communs, conformément à la norme ISO/IEC 15408, ou la validation FIPS 140-2;

f) Un graphique détaillé du réseau.

2.11.4 Procédures d'exploitation de la sécurité

(28) L'entrepreneur doit fournir au Canada ses procédures d'exploitation de la sécurité décrivant ce qui suit :

a) Les exigences de renforcement des systèmes s'appliquant aux serveurs, entrepôts de données, dispositif de réseau et applications, ainsi que les procédures de vérification du renforcement;

b) Les fonctions de l'environnement d'exploitation, notamment :

i) La séquence de mise sous tension et de mise hors tension;

ii) L'utilisation de comptes de système privilégiés;

iii) Le démarrage et la fermeture des systèmes (y compris du système d'exploitation et des applications);

iv) Le début et la fin des communications;

v) La sauvegarde et la restauration;

vi) La dérogation aux contrôles de sécurité (le cas échéant);

vii) La reprise ou le redémarrage;

c) Les procédures et les mesures prioritaires d'intervention en cas d'incident, afin d'atténuer le préjudice, de contenir les causes des incidents et de rétablir les services, y compris la notification au Canada;

d) Les types d'événements ou d'activités qui constituent un incident de sécurité, les incidents de sécurité des TI pouvant survenir, leur incidence éventuelle, l'environnement technique et opérationnel, et les priorités en matière de prestation de services s'appliquant, au minimum, aux incidents de sécurité indiqués ci-après :

i) Les cybermenaces;

ii) Les logiciels malveillants;

iii) Les virus;

iv) Les vers informatiques;

v) Les chevaux de Troie;

vi) Les trappes;

vii) Les programmes malveillants furtifs;

viii) Les enregistreurs de frappe;

ix) Les réseaux de zombies;

x) L'hameçonnage;

xi) Les attaques par script intersites (cross site scripting [XSS]));

xii) La mystification;

xiii) La dégradation de sites Web;

xiv) La contamination des systèmes/sites;

xv) La compromission des systèmes/sites;

xvi) La compromission des systèmes/justificatifs d'utilisateur;

xvii) Le déni de service;

xviii) Le déni de service distribué;

xix) Le vol;

xx) Les pourriels;

xxi) Les attaques du jour zéro;

xxii) Les atteintes à la vie privée;

xxiii) Les exploits;

xxiv) Les cyberattaques;

xxv) L'exfiltration de données;

xxvi) Les activités de reconnaissance;

xxvii) Les injections;

xxviii) Les requêtes illégitimes entre sites;

xxix) Les infractions aux politiques relatives aux services de gestion des menaces;

e) Le protocole en cas d'atteinte à la vie privée, y compris sans s'y limiter, les processus de notification pertinents;

f) Les processus visant à surveiller les vulnérabilités visant la sécurité des systèmes et à appliquer les correctifs de sécurité en conséquence.

(29) L'entrepreneur doit établir l'ordre de priorité, le temps de réponse et le délai de notification associés aux processus des services de gestion, pour les incidents de sécurité en fonction d'une échelle de gravité comportant des normes relatives au temps de réponse fournie par le Canada.

2.11.5 Matrice de traçabilité des exigences de sécurité

(30) L'entrepreneur doit fournir au Canada une matrice de traçabilité des exigences de sécurité (MTES) qui prévoit, pour chaque exigence d'assurance de la sécurité du SSGGC marquée aux fins de validation dans la matrice pour la certification de la sécurité de l'appendice B de l'annexe A au SSGGC, des renvois à la conception du service qui décrivent les mécanismes de sécurité à mettre en œuvre à l'égard de chaque exigence. La MTES fournit l'assurance que la conception du SSGGC satisfait pleinement à ses exigences de sécurité.

(31) En plus de la MTES, il faut fournir au Canada tous les documents portant sur le service qui y sont mentionnés; ces documents doivent décrire les mécanismes de sécurité de façon suffisamment détaillée pour permettre au Canada de confirmer que ces mécanismes satisfont aux exigences de sécurité marquées aux fins de validation dans la matrice pour la certification de la sécurité de l'appendice B de l'annexe A au SSGGC.

2.11.6 Vérification de la sécurité

(32) L'entrepreneur doit fournir au Canada un plan de test de vérification de la sécurité qui documente les jeux d'essai destinés à vérifier chaque exigence d'assurance de la sécurité du SSGGC, marquée aux fins de vérification de la sécurité dans la matrice pour la certification de la sécurité de l'appendice B de l'annexe A au SSGGC.

(33) L'entrepreneur doit exécuter le plan de test de vérification de la sécurité et fournir au Canada un rapport de vérification de la sécurité qui intègre, pour chaque mécanisme de sécurité qui satisfait à au moins une des exigences de sécurité marquées aux fins de vérification de la sécurité dans la matrice pour la certification de la sécurité de l'appendice B de l'annexe A au SSGGC, les éléments suivants :

a) La procédure de vérification de la sécurité visant à confirmer que le mécanisme de sécurité est mis en œuvre correctement et satisfait aux normes applicables précisées dans les spécifications de conception du service;

b) Les résultats prévus et réels pour chaque procédure de vérification de la sécurité;

c) Pour chaque écart par rapport aux résultats prévus, qui a pu être corrigé au moment de la vérification, une description des mesures correctives mises en œuvre dans le SSGGC;

d) Les documents portant sur le service mentionnés dans la MTES et devant être mis à jour par suite de la mise en œuvre des mesures correctives;

e) Pour chaque écart par rapport aux résultats prévus, qui n'a pu être corrigé au moment de la vérification (p. ex. en raison de changements plus importants), indiquer l'écart dans le plan de traitement des risques.

(34) L'entrepreneur doit mettre à jour la MTES pour y inclure le traçage entre les exigences de sécurité marquées aux fins de vérification de la sécurité et les procédures de vérification de la sécurité.

(35) L'entrepreneur doit fournir au Canada la MTES mise à jour.

(36) L'entrepreneur doit permettre au Canada d'assister aux tests de vérification de la sécurité en lui permettant :

a) D'accéder physiquement à ses installations où a lieu la mise en œuvre du SSGGC;

b) D'observer ses représentants pendant qu'ils exécutent les procédures de vérification de la sécurité.

2.11.7 Test de sécurité

(37) L'entrepreneur doit fournir au Canada un plan de test de sécurité qui documente les jeux d'essai destinés à vérifier chaque exigence d'assurance de la sécurité du SSGGC, marquée aux fins de test de sécurité dans la matrice pour la certification de la sécurité de l'appendice B de l'annexe A au SSGGC.

(38) L'entrepreneur doit exécuter le plan de test de sécurité et fournir au Canada un rapport de test de sécurité qui intègre, pour chaque mécanisme de sécurité qui satisfait à au moins une des exigences de sécurité marquées aux fins de test de sécurité dans la matrice pour la certification de la sécurité de l'appendice B de l'annexe A au SSGGC, les éléments suivants :

a) La procédure de test de sécurité visant à confirmer que le mécanisme de sécurité est mis en œuvre correctement et satisfait aux normes applicables précisées dans les spécifications de conception du service;

b) Les résultats prévus et réels pour chaque procédure de test de sécurité;

c) Pour chaque écart par rapport aux résultats prévus, qui a pu être corrigé au moment de la vérification, une description des mesures correctives mises en œuvre dans le SSGGC;

d) Les documents portant sur le service mentionnés dans la MTES et devant être mis à jour par suite de la mise en œuvre des mesures correctives;

e) Pour chaque écart par rapport aux résultats prévus, qui n'a pu être corrigé au moment de la vérification (p. ex. en raison de changements plus importants), indiquer l'écart dans le plan de traitement des risques.

(39) L'entrepreneur doit mettre à jour la MTES pour y inclure le traçage entre les exigences de sécurité marquées aux fins de test de sécurité et les procédures de test de sécurité.

(40) L'entrepreneur doit fournir au Canada la MTES mise à jour.

(41) L'entrepreneur doit permettre au Canada d'assister aux tests de sécurité en lui permettant :

a) D'accéder physiquement à ses installations où a lieu la mise en œuvre du SSGGC;

b) D'observer ses représentants pendant qu'ils exécutent les procédures de test de sécurité.

2.11.8 Évaluation et atténuation des vulnérabilités

(42) L'entrepreneur doit permettre au Canada d'effectuer une évaluation de la vulnérabilité par rapport au SSGGC qui prévoit :

a) L'accès physique à ses installations où l'infrastructure (matériel, logiciels) du SSGGC est située;

b) L'accès réseau au SSGGC pour permettre le balayage du réseau et des dispositifs hôte;

c) La présence d'au moins une ressource technique qui connaît les aspects techniques du SSGGC (matériel, logiciels, et produits de réseau et leur configuration), pour prêter assistance pendant la durée du volet « sur place » de l'évaluation de la vulnérabilité.

(43) Le Canada peut effectuer une évaluation de la vulnérabilité par rapport au SSGGC et fournir à l'entrepreneur un rapport d'évaluation dans lequel il indiquera les vulnérabilités qu'il a détectées. Le Canada restreindra son évaluation aux activités de découverte et de balayage et ne s'engagera pas dans des activités perturbatrices ou destructrices.

(44) Le Canada peut aussi, à sa discrétion, demander à l'entrepreneur d'effectuer les tests d'évaluation de la vulnérabilité en se servant d'un plan qu'il a approuvé et de lui soumettre les résultats pertinents.

(45) L'entrepreneur doit fournir au Canada un rapport d'atténuation de la vulnérabilité comprenant ce qui suit :

a) Une liste des vulnérabilités pour lesquelles le Canada recommande la mise en œuvre de mesures correctives;

b) Une description des mesures correctives à mettre en œuvre, y compris les délais prévus;

c) Les documents portant sur le service mentionnés dans la MTES et devant être mis à jour par suite de la mise en œuvre des mesures correctives.

2.11.9 Plan de traitement des risques

(46) L'entrepreneur doit fournir au Canada un plan de traitement des risques visant le suivi et le traitement des questions en suspens suivantes :

a) Les risques encourus lorsque les exigences de sécurité ou les exigences fonctionnelles ne sont pas satisfaites;

b) Les écarts notés lors du test de vérification de la sécurité et devant être corrigés;

c) Les écarts notés lors du test de sécurité et devant être corrigés;

d) Les mesures correctives indiquées dans le rapport d'atténuation de la vulnérabilité.

(47) Pour chaque mesure corrective, le plan de traitement des risques doit comprendre les renseignements suivants :

a) La personne responsable de la mise en œuvre de la mesure;

b) Le délai visé pour l'atténuation des risques (date et version);

c) Une évaluation du risque résiduel une fois la mesure mise en œuvre;

d) Le niveau de priorité établi par le Canada pour la mise en œuvre de chacune des mesures.

(48) L'entrepreneur doit exécuter les travaux relatifs au plan de traitement des risques, selon un plan approuvé par le Canada à la suite de la mise en œuvre du SSGGC et qui stipule que l'exécution des travaux ne doit pas dépasser 120 JOFPF.

(49) L'entrepreneur doit fournir, dans les 20 JOFPF suivant l'achèvement du plan de traitement des risques, un rapport qui présente tous les résultats des tests afin de vérifier l'efficacité des mesures correctives mises en œuvre.

2.12 Mise en œuvre du SSGGC

(50) L'entrepreneur doit fournir et entretenir les composantes matérielles et logicielles relatives au SSGGC.

(51) L'entrepreneur doit mettre en œuvre le SSGGC dans un ou plusieurs PPS du Canada, au Canada, selon ce que précise celui-ci.

(52) Les services de gestion des menaces du SSGGC doivent interagir de façon uniforme, sans se nuire l'un l'autre, comme une seule entité logique.

(53) La performance d'un service de gestion des menaces du SSGGC ne doit pas se répercuter sur le rendement des autres services de gestion des menaces du SSGGC faisant partie d'une capacité de gestion des menaces du SSGGC.

(54) Le SSGGC doit permettre la combinaison de multiples capacités de gestion des menaces à un PPS afin d'atteindre une vitesse filaire combinée.

(55) Les capacités combinées de gestion des menaces du SSGGC, offertes à un PPS, doivent interagir de façon uniforme, sans se nuire l'une l'autre, comme une capacité unique de gestion des menaces du SSGGC.

(56) Les services de gestion des menaces du SSGGC doivent prendre en charge au moins des configurations uniques des organisations clientes qui fonctionnent de façon indépendante sans se nuire l'une l'autre.

(57) Le SSGGC doit permettre la combinaison de multiples capacités en matière de GIES à un PPS donné afin d'atteindre le taux combiné de transactions par seconde (TPS).

(58) Les capacités combinées du SSGGC en matière de GIES, offertes à un PPS, doivent interagir de façon uniforme, sans se nuire l'une l'autre, comme une capacité unique du SSGGC en matière de GIES.

(59) L'entrepreneur doit commencer à rendre compte des niveaux de service et de la performance du SSGGC immédiatement après son acceptation par le Canada.

(60) L'entrepreneur doit mettre en œuvre le SSGGC, conformément à ce qui suit :

a) La conception du service (voir la sous-section Conception du service);

b) Les exigences de sécurité (voir l'appendice A – Exigences de sécurité de l'annexe A au SSGGC);

c) L'architecture de sécurité (voir la sous-section Architecture de sécurité);

d) Les procédures d'exploitation de la sécurité (voir la sous-section Procédures d'exploitation de la sécurité);

e) Le bulletin de sécurité TI ITSB-60 : *Conseils sur l'utilisation du protocole TLS (Transport Layer Security) au sein du gouvernement du Canada* (http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb60-fra.html);

f) Le bulletin de sécurité TI ITSB-61 : *Conseils sur l'utilisation du protocole de sécurité IP (IPsec) au sein du gouvernement du Canada* (http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb61-fra.html);

g) Les normes de la Normalisation des sites Internet du gouvernement du Canada (version 2.0) publiées par le Secrétariat du Conseil du Trésor du Canada (http://www.tbs-sct.gc.ca/clf2-nsi2/index-fra.asp);

h) Les règles pour l'accessibilité des contenus Web 2.0 (WCAG 2.0) de W3C, niveau AA, directives 1 et 2 (http://www.w3.org/Translations/WCAG20-fr/);

i) La *Politique sur le programme de coordination de l'image de marque* (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12314);

j) La *Politique de communication du gouvernement du Canada* (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12316);

k) *La Loi sur les langues officielles* du Canada *(*http://lois.justice.gc.ca/fra/O-3.01).

2.12.1 Amélioration du service

(61) Si de nouveaux services de gestion des menaces devaient être offerts, le Canada et l'entrepreneur examineront s'il y a lieu de les intégrer au SSGGC, et ils pourraient parvenir à une entente à cet égard.

2.12.2 Sécurité

(62) Le logiciel du SSGGC, tel qu'il est décrit dans la conception du service, doit être assorti d'une certification d'au moins EAL-4 selon les Critères communs.

(63) Les produits cryptographiques (modules logiciels, ICP, jetons d'authentification et autres, au besoin) employés par le SSGGC, tels qu'ils sont indiqués dans la conception du service, doivent respecter les exigences suivantes :

a) Utiliser des algorithmes et des tailles de clé approuvés par le CSTC, validés par le Programme de validation des modules cryptographiques (http://csrc.nist.gov/groups/STM/cavp/) et mentionnés dans l'alerte de sécurité des TI ITSA-11E (http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11e-fra.html) ou dans une alerte subséquente;

b) Être mis en œuvre dans un module cryptographique et validés par le Programme de validation des modules cryptographiques (http://www.cse-cst.gc.ca/its-sti/services/industry-prog-industrie/cmvp-pvmc-fra.html) à tout le moins au niveau 1 de la norme FIPS 140-2;

c) Fonctionner en mode FIPS.

2.12.3 Connectivité de réseau

(64) Le SSGGC doit se conformer aux normes de réseau qui suivent (telles qu'elles sont détaillées dans la section Normes) :

a) Protocole Internet.

(65) Le SSGGC doit fournir au moins deux interfaces réseau pour chaque composante matérielle associée à une capacité de gestion des menaces du SSGGC, à un site du Canada pouvant être relié à un service de réseau du Canada, précisé par le Canada, qui prend en charge les normes de réseau qui suivent (voir la section Normes) :

a) Ethernet rapide;

b) Gigabit Ethernet.

(66) Le SSGGC offert à un PPS doit automatiquement transférer le trafic, y compris le trafic compatible avec la session, au SSGGC à un PPS de secours que précise le Canada à la suite de la défaillance du SSGGC à un PPS donné, lorsque le transfert du trafic existant compatible avec la session se fait d'une manière si transparente que l'utilisateur ne perd pas sa session.

(67) Le SSGGC ne doit pas avoir d'effet sur la performance des accélérateurs Web du Canada.

2.12.4 Performance

(68) La capacité de gestion des menaces du SSGGC doit traiter les paquets selon des vitesses filaires soutenues dans les deux directions simultanément, peu importe le nombre de services de gestion des menaces du SSGGC en exploitation simultanément et le contenu des paquets.

(69) La capacité du SSGGC en matière de GIES doit traiter les transactions selon le taux de TPS soutenu, peu importe le contenu ou la taille des transactions.

2.12.5 Journalisation

(70) La journalisation des événements du SSGGC doit viser au minimum les données nécessaires aux fins suivantes :

a) La production de rapports;

b) La réalisation d'analyse en informatique judiciaire;

c) La détermination des niveaux de service;

d) L'utilisation du service;

e) La gestion du service;

f) La gestion de la sécurité;

g) L'exécution des activités du service.

(71) Le SSGGC doit permettre la capture intégrale des paquets.

(72) Le SSGGC doit fournir la journalisation des événements en double, dans les cinq minutes suivant l'apparition d'un événement, dans un format compatible avec la version 1.2 du protocole d'automatisation de contenu de sécurité (SCAP), à un GIES du

SSGGC ou à un GIES du Canada, tel que le précise le Canada en fonction de chaque organisation cliente.

(73) Le SSGGC doit offrir la journalisation des événements en double, dans les cinq minutes suivant l'apparition d'un événement, par un serveur syslog du Canada, dans un format compatible avec la version 1.2 du protocole SCAP, tel que le précise le Canada en fonction de chaque organisation cliente.

2.12.6 Portail de services

(74) L'entrepreneur doit fournir un point central d'accès sécurisé à toute l'information (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC et l'administration de celui-ci; ce portail de services doit être accessible au moyen d'un navigateur Web.

(75) L'entrepreneur doit fournir les comptes d'accès, pour permettre aux utilisateurs autorisés d'accéder à l'information (rapports, données, documents, journaux, configurations, etc.) concernant le SSGGC et aux fonctions d'administration du portail de services, dans les deux JOFPF suivant une demande présentée par le Canada.

(76) Le portail de services doit authentifier les utilisateurs à l'aide d'un service d'authentification axé sur les certificats X.509 fourni par le Canada, selon ce qu'il précise.

(77) L'entrepreneur doit appliquer l'interface entre le portail de services et le service d'authentification fourni par le Canada.

(78) L'entrepreneur doit fournir au Canada un portail de services comprenant ce qui suit :

a) L'accès au moyen d'un navigateur Web pour au moins 50 utilisateurs simultanés;

b) L'accès HTTPS à l'aide de certificats approuvés par le navigateur Web;

c) L'accès aux seuls utilisateurs autorisés par le Canada;

d) L'accès aux seuls utilisateurs authentifiés à l'aide d'un justificatif approuvé par le Canada;

e) La désactivation automatique des utilisateurs inactifs, à l'aide d'une méthode approuvée par le Canada;

f) Une page d'orientation/d'introduction;

g) L'aide en ligne et les coordonnées pertinentes de sa personne-ressource;

h) La recherche, la visualisation et le téléchargement de l'état des billets de changement et d'incident (y compris les fichiers journaux);

i) La recherche, la visualisation et le téléchargement de documents;

j) La recherche, la visualisation et le téléchargement de configurations;

k) La recherche et la visualisation des autorisations de tâches, et l'examen de leur état;

l) L'accès par Internet;

m) Une interface conviviale dotée de menus et d'options en langage clair et simple et structurés logiquement;

n) L'entrée de données assistée où des zones d'entrée contenant des valeurs prédéfinies sont remplies au moyen de listes, déroulantes ou non, de cases à cocher et de boutons radio présentés en langage clair et simple;

o) L'entrée de données assistée où les champs d'entrée sont composés (c'est-à-dire où de multiples éléments de données sont concaténés à l'intérieur du même champ d'entrée); ces zones seraient remplies à l'aide d'une combinaison de listes, déroulantes ou non, de cases à cocher et de boutons radio, présentés en langage clair et simple, pour les valeurs prédéfinies, et de boîtes de texte pour les valeurs fournies par l'utilisateur;

p) La vérification des erreurs lorsque les zones d'entrée sont examinées pour en confirmer le format ou la validité, y compris la validation croisée des zones; les messages d'erreur sont détaillés, rédigés en langage clair et simple et indiquent à l'utilisateur ce qui est incorrect et les règles qui n'ont pas été satisfaites;

q) Des zones prédéfinies (p. ex. service, PPS, type de travail, nom de la personne-ressource, prix unitaire, numéro d'article, quantité, etc.) approuvées par le Canada, dont l'entrée de données est assistée (s'il y a lieu) pour réduire au minimum les entrées fautives.

(79) Le portail de services ne doit pas exiger le recours aux éléments ActiveX pour accéder à l'information concernant le SSGGC.

(80) L'entrepreneur doit appliquer un processus de gestion des changements et des mises en production à l'égard des changements et des mises en production liés au portail de services, et au sujet de tout changement apporté aux systèmes et services accessibles par celui-ci.

(81) L'entrepreneur doit fournir au Canada une notification de mise en production dans les cinq JOFPF précédant tout changement ou toute mise en production liés au portail de services.

(82) L'entrepreneur doit fournir au Canada un exemplaire électronique d'un guide de l'utilisateur du portail de services à la suite de la mise en œuvre du portail de services; ce guide contiendra des renseignements sur ce qui suit :

a) Les instructions concernant la structure, le contenu et l'utilisation du portail de services;

b) Les copies d'écran concernant les menus, les entrées de données et les rapports;

c) Le processus de gestion des changements et des mises en production liés au portail de services.

(83) L'entrepreneur doit sauvegarder quotidiennement toute l'information (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC accessible au moyen du portail de services; il doit conserver ces sauvegardes quotidiennes hors site pendant une période de trois ans.

(84) Le portail de services doit fournir l'accès en ligne (soit directement comme fonctionnalité inhérente au portail, soit indirectement au moyen d'un lien) à toute l'information (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC pour les trois années précédentes.

(85) Toutes les fonctions d'administration, toute la documentation et tous les rapports fournis au Canada à l'égard des services gérés du SSGGC doivent être accessibles au moyen du portail de services, à moins d'indication contraire du Canada.

(86) L'entrepreneur ne doit résumer, à l'égard du SSGGC, que les données (sommes, moyennes, etc.) approuvées par le Canada.

(87) L'entrepreneur doit archiver toute l'information (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC qui date de plus de 3 ans; cette information est accessible à l'aide du portail de services pendant toute la durée du contrat. De plus, il doit fournir l'information que demande le Canada sur le SSGGC sur un support que précise le Canada, dans un format de fichier commercial approuvé par le Canada, et ce, dans les 10 JOFPF suivant une demande à cet effet.

(88) L'entrepreneur doit déterminer les temps de réponse maximaux (période de demande moyenne et de pointe) applicables à l'obtention de renseignements (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC de la part du portail de services, en se servant de repères approuvés par le Canada.

(89) Les temps de réponse maximaux visant le portail de services ne doivent pas être supérieurs à trois secondes pendant plus de trois minutes (soit l'équivalent approximatif de 5,00 % du temps) au cours de chaque heure (p. ex. de 7 h à 8 h HE) de chaque JOFPF, entre 7 h et 19 h HE pour chaque jour au cours d'un mois civil.

(90) Le portail de services doit répondre aux demandes d'information (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC dans un délai inférieur ou égal aux temps de réponse maximaux.

(91) L'entrepreneur doit mesurer, toutes les heures, les temps de réponse s'appliquant au portail de services.

(92) Le portail de services doit fournir, à un utilisateur authentifié, l'accès à toutes les pages ou fonctions du portail de services auxquelles il est autorisé à accéder, sans que cet utilisateur ait à s'authentifier de nouveau après son authentification initiale, et ce, jusqu'à ce qu'il ferme sa session ou que celle-ci expire.

(93) Le portail de services doit consigner tous les accès au portail de services et fournir au Canada un fichier électronique des enregistrements visant les accès effectués au cours des 12 mois précédents, et ce, en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada.

(94) Le portail de services doit comprendre les profils d'accès qui permettent au Canada de définir les droits (lire/visualiser; écrire/modifier; supprimer; télécharger) qu'a un utilisateur lorsqu'il accède :

a) Aux pages du portail de services et aux champs contenus dans une page du portail de services;

b) À l'information (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC accessible à l'aide du portail de services.

(95) Le portail de services doit comprendre les groupes d'accès qui permettent au Canada de déterminer les groupes d'utilisateurs qui ont accès au portail de services.

(96) Le portail de services doit permettre au Canada d'attribuer un profil d'accès à un groupe d'accès de sorte que tous les utilisateurs faisant partie d'un groupe d'accès donné disposent des droits d'accès, selon ce qu'indique le profil d'accès connexe.

(97) Le portail de services doit permettre l'autoenregistrement en ligne des utilisateurs, notamment :

a) La saisie d'information liée au profil utilisateur;

b) La prévention de tentatives d'enregistrement non autorisées;

c) L'examen des demandes d'enregistrement en ligne et leur approbation par le Canada;

d) L'attribution de profils d'accès;

e) L'envoi automatique d'un courriel à l'utilisateur après que son enregistrement a été approuvé.

(98) Les profils utilisateur du portail de services doivent comprendre ce qui suit :

a) L'ID de justificatif de l'utilisateur;

b) L'adresse de courriel;

c) L'emplacement du PPS (ex. adresse);

d) Les coordonnées téléphoniques;

e) La préférence linguistique (français ou anglais);

f) Le nom de l'organisation cliente.

(99) Le portail de services doit permettre la gestion libre-service des profils en vertu de laquelle l'utilisateur pourra gérer des éléments approuvés de son profil utilisateur.

(100) Le portail de services doit afficher le texte ou les pages d'aide, et le texte ou les commandes de navigation, dans la langue préférée (français ou anglais) de l'utilisateur précisée dans son profil utilisateur.

(101) Le portail de services doit permettre à l'utilisateur de changer la préférence linguistique afin que le portail affiche le texte ou les pages d'aide, et le texte ou les commandes de navigation, dans l'autre langue.

(102) Le portail de services doit permettre au Canada de trier les résultats des rapports sous forme de tableau selon le ou les champs précisés par l'utilisateur.

(103) Le portail de services doit permettre au Canada de télécharger les rapports en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada.

(104) Le portail de services doit permettre au Canada de télécharger les données de base servant à la production des rapports, en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada.

(105) Le portail de services doit permettre au Canada de créer de manière dynamique des rapports sous forme de tableau qui prévoient notamment :

a) La sélection des sources de données disponibles;

b) Le jumelage de multiples sources de données selon les champs sélectionnés;

c) La sélection des champs à l'intérieur des sources de données;

d) La détermination des critères de sélection pour les champs sélectionnés;

e) La sélection des champs devant figurer dans le rapport;

f) L'attribution implicite de la valeur des en-têtes de colonne au nom du champ;

g) La disposition des champs dans le rapport;

h) La création de champs calculés au moyen d'opérations mathématiques dans d'autres champs;

i) La création de champs calculés à l'aide de fonctions intégrées comme l'établissement de la somme, du compte total, de la moyenne, du nombre maximal, du nombre minimal, etc.;

j) La détermination de l'ordre de tri dans le rapport;

k) La détermination des champs devant servir pour le total partiel et du type de total partiel (p. ex. somme ou compte total);

l) La modification par l'utilisateur des en-têtes par défaut des rapports et des colonnes;

m) La sauvegarde par l'utilisateur du modèle du rapport sous un nom qu'il précise;

n) L'extraction par l'utilisateur du modèle du rapport par nom de rapport;

o) La modification par l'utilisateur du modèle de rapport;

p) L'exécution du rapport par l'utilisateur.

(106) Le portail de services doit permettre au Canada d'insérer dans le rapport un graphique qui prévoit notamment :

a) La sélection des colonnes du rapport afin d'y inclure des séries de données;

b) La sélection du type de graphique :

i) Graphique à colonnes;

ii) Graphique circulaire;

iii) Graphique à bandes;

iv) Graphique linéaire;

v) Graphique de surface;

c) Le formatage du graphique, y compris :

i) Des séries de données;

ii) Du type de présentation (valeurs ou pourcentages);

iii) Des couleurs;

iv) Des étiquettes;

v) Des titres.

(107) Le portail de services doit permettre au Canada de visualiser les registres disponibles par organisation cliente, dispositif, date, numéro de billet d'incident ou de toute autre métadonnée connexe.

(108) Le portail de services doit publier les registres au plus tard à 9 h HE le prochain jour civil.

(109) Le portail de services doit permettre à un utilisateur privilégié d'accéder en temps réel à n'importe quelle plateforme de service du SSGGC et de :

a) Visualiser les entrées du registre;

b) Rechercher les entrées du registre;

c) Télécharger les registres en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada;

d) Visualiser la configuration de la plateforme et des services;

e) Télécharger les configurations en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada.

(110) Le portail de services doit permettre au Canada de télécharger les registres en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada.

(111) Le portail de services doit afficher un qualificatif indiquant que l'information concernant le SSGGC est chiffrée, et il ne doit pas afficher l'information à moins que l'utilisateur ne fournisse la clé de déchiffrement nécessaire.

(112) Le portail de services doit permettre seulement le téléchargement de l'information chiffrée concernant le SSGGC en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada.

(113) L'entrepreneur doit créer des comptes d'administrateur du portail de services, à la demande du Canada.

(114) Le portail de services doit autoriser l'administration déléguée du portail de services en permettant à un de ses administrateurs de visualiser, créer, modifier et supprimer les comptes d'administrateur délégué.

(115) Le portail de services doit permettre à un administrateur ou un administrateur délégué :

a) De visualiser, créer, modifier et supprimer :

i) Les comptes d'utilisateur;

ii) Les profils d'accès;

iii) Les groupes d'accès;

b) De réactiver ou de désactiver les comptes d'utilisateur;

c) D'autoriser les demandes d'autoenregistrement des utilisateurs;

d) D'interroger, trier et visualiser les profils utilisateur selon tout champ figurant dans le profil;

e) De télécharger les résultats de l'interrogation des profils utilisateur en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada.

(116) Le portail de services doit fournir, pour chaque organisation cliente, une vue accessible uniquement par les utilisateurs de cette organisation; cette vue est déterminée par le Canada et fournit l'accès à ce qui suit :

a) Une page d'orientation de l'organisation cliente comprenant :

i) Des pages de navigation et d'aide;

ii) Des liens vers les sites externes que précise le Canada;

iii) L'identification des fonctionnalités courantes du portail de services;

iv) Une fonction de recherche de l'information figurant dans le portail de services;

v) Une description de l'organisation de l'entrepreneur et ses coordonnées;

vi) Une carte du site Web;

b) Uniquement l'information (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC associée à l'organisation cliente. Par exemple,

l'utilisateur d'une organisation cliente ne doit être en mesure de visualiser que les incidents, autorisation de tâches, registres, rapports, etc., applicables à cette organisation.

(117) Le portail de services doit offrir une vue qui n'est accessible que par les administrateurs et qui comprend :

i) Des pages de navigation et d'aide;

ii) Des liens vers les sites externes que précise le Canada;

iii) L'identification des fonctionnalités courantes du portail de services;

iv) Une fonction de recherche de l'information figurant dans le portail de services;

v) Une description de l'organisation de l'entrepreneur et ses coordonnées;

vi) Une carte du site Web;

vii) L'accès à l'information (données, rapports, documents, journaux, configurations, etc.) concernant le SSGGC applicable à l'ensemble des organisations clientes.

2.12.7 Pare-feu

(118) Le pare-feu agit comme un mécanisme de protection des actifs informationnels du Canada contre les menaces électroniques provenant de l'intérieur de gouvernement du Canada, ainsi que celles attribuables à la connexion à un réseau non fiable, tel Internet.

(119) Les exigences de l'Énoncé des travaux concernant le pare-feu sont définies dans l'annexe A-1 : Énoncé des travaux – Pare-feu au SSGGC.

2.12.8 Prévention et détection des intrusions

(120) La prévention et la détection des intrusions (PDI) surveillent le trafic réseau du Canada en temps réels en vue de déceler une activité hostile et d'alerter celui-ci dès que possible au sujet d'atteintes à la sécurité ou d'attaques organisées, et prennent les mesures appropriées.

(121) Les exigences de l'Énoncé des travaux concernant la PDI sont définies dans l'annexe A-2 : Énoncé des travaux – Prévention et détection des intrusions au SSGGC.

2.12.9 Filtrage de contenu

(122) Le filtrage de contenu balaie les demandes et le trafic Internet et peut empêcher l'accès à des sites et à du contenu Internet indésirables au moyen de politiques normalisées, appuyant ainsi la politique du Canada en matière d'utilisation acceptable.

(123) Les exigences de l'Énoncé des travaux concernant le filtrage de contenu sont définies dans l'annexe A-3 : Énoncé des travaux – Filtrage de contenu au SSGGC.

2.12.10 Antivirus

(124) L'antivirus assure une protection contre les codes malveillants en filtrant le trafic entrant et sortant afin de bloquer les fichiers infectés.

(125) Les exigences de l'Énoncé des travaux concernant l'antivirus sont définies dans l'annexe A-4 : Énoncé des travaux – Antivirus au SSGGC.

2.12.11 Antipourriel

(126) L'antipourriel assure le captage des pourriels entrants et sortants en vue du filtrage et du blocage des tentatives d'hameçonnage.

(127) Les exigences de l'Énoncé des travaux concernant l'antipourriel sont définies dans l'annexe A-5 : Énoncé des travaux – Antipourriel au SSGGC.

2.12.12 Prévention des pertes de données

(128) La prévention des pertes de données (PPD) décèle, surveille et protège les données lors d'activités d'extrémité et de réseau afin de détecter et de prévenir toute transmission et utilisation non autorisées de renseignements confidentiels tout en renforçant les politiques internes connexes.

(129) Les exigences de l'Énoncé des travaux concernant le PPD sont définies dans l'annexe A-6 : Énoncé des travaux – Prévention des pertes de données au SSGGC.

2.12.13 Gestion des informations et des événements de sécurité

(130) La gestion des informations et des événements de sécurité (GIES) collecte, analyse et corrèle l'information de journaux provenant de nombreuses sources à l'échelle de l'organisation, y compris de capteurs placés à des endroits stratégiques, afin de fournir des renseignements au sujet d'événements et d'incidents critiques liés à la sécurité tout en assurant l'établissement de documents et de rapports de nature judiciaire.

(131) Les exigences de l'Énoncé des travaux concernant la GIES sont définies dans l'annexe A-7 : Énoncé des travaux – Gestion des informations et des événements de sécurité au SSGGC.

3 GESTION DU SERVICE

(132) L'entrepreneur doit désigner un gestionnaire opérationnel qui agira en tant que seul point de contact quotidien pour le Canada pour la gestion du service; ce gestionnaire doit être en mesure de rencontrer en personne les représentants du Canada dans la région de la capitale nationale (RCN) entre 8 h et 17 h HE, pendant les JOFPF.

(133) L'entrepreneur doit désigner un gestionnaire du service qui servira de point de contact et agent de liaison initial pour le Canada pour les éléments suivants, sans s'y limiter :

a) La signalisation des incidents, y compris des incidents de sécurité;

b) L'analyse des causes fondamentales (ACF);

c) Les niveaux de service;

d) Les activités de mise en œuvre;

e) L'établissement du calendrier concernant les périodes de maintenance et de mises en production;

f) La qualité du service;

g) L'assurance du service;

h) La consultation concernant le service;

i) Les rapports sur le service;

j) La disponibilité et la performance du service;

k) Les processus du service.

(134) Le gestionnaire du service, ou son délégué autorisé, doit répondre aux appels et aux courriels des représentants du Canada en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année).

(135) Le gestionnaire du service doit être en mesure de rencontrer en personne les représentants du Canada dans la RCN entre 8 h et 17 h HE pendant les JOFPF, et ce, dans les deux JOFPF suivant une demande présentée par le Canada.

(136) L'entrepreneur doit désigner un architecte du service qui servira de point de contact unique pour le Canada pour les éléments suivants :

a) La planification, la conception et l'ingénierie;

b) L'analyse des exigences et des incidences;

c) La détermination des changements et les recommandations à cet égard.

(137) L'architecte du service doit être en mesure de rencontrer en personne les représentants du Canada dans la RCN entre 8 h et 17 h HE pendant les JOFPF, et ce, dans les deux JOFPF suivant une demande présentée par le Canada.

(138) L'entrepreneur doit désigner un spécialiste des opérations et des mesures d'intervention de sécurité qui servira de point de contact pour le Canada pour les éléments suivants :

a) Les incidents de sécurité;

b) Les problèmes de sécurité;

c) Les demandes d'information portant sur la sécurité;

d) La coordination des mesures d'intervention de sécurité;

e) Les alertes de sécurité.

(139) L'entrepreneur doit désigner un spécialiste des opérations et des mesures d'intervention de sécurité qui possède les qualifications minimales suivantes :

a) Expérience pertinente liée aux mesures d'intervention et aux opérations de sécurité;

b) Connaissance approfondie de la solution SSGGC;

c) Capacité d'analyse et d'évaluation rapides des données relative à un incident;

d) Capacité de fournir une évaluation factuelle de la situation;

e) Formation complète dans l'application de la solution de surveillance de la sécurité et d'établissement de rapports du SSGGC;

f) Capacité de répondre rapidement aux demandes d'information;

g) Axé sur la clientèle;

h) Capacité de travailler en situation urgente ou très stressante;

i) Bilinguisme.

(140) Le spécialiste des opérations et des mesures d'intervention de sécurité, ou son délégué autorisé, doit répondre aux appels et aux courriels des représentants du Canada en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année).

3.1 Centre des opérations

(141) L'entrepreneur doit fournir un centre principal des opérations 24 heures sur 24, sept jours sur sept, 365 jours par année; ce centre sera doté de l'infrastructure et des ressources nécessaires pour assurer l'exploitation et la gestion centralisées du SSGGC.

(142) L'entrepreneur doit également fournir un centre des opérations de secours qui, sans être situé physiquement dans les mêmes installations (c'est-à-dire même immeuble) que le centre principal des opérations, offre toutes les fonctionnalités opérationnelles et de gestion prises en charge par ce centre.

(143) La transition du centre principal des opérations vers le centre des opérations de secours doit se faire de façon transparente pour le Canada et ne doit pas avoir d'incidence sur les opérations du SSGGC.

(144) L'entrepreneur doit effectuer la transition du centre principal des opérations vers le centre des opérations de secours, conformément au plan de continuité du service.

(145) L'entrepreneur doit mettre à l'essai chaque année la transition du centre principal des opérations vers le centre des opérations de secours et fournir au Canada un rapport contenant les résultats de l'essai et les recommandations pertinentes.

(146) Le centre des opérations doit surveiller les incidents en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année).

(147) L'entrepreneur doit fournir les composantes matérielles et logicielles nécessaires à la surveillance, à la compilation, à l'analyse et à la déclaration des incidents.

3.2 Centre des opérations de sécurité de l'information

(148) L'entrepreneur doit fournir en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année) un centre des opérations de sécurité de l'information (COSI) principal doté de l'infrastructure et des ressources nécessaires pour assurer la surveillance centralisée des alarmes et conditions du SSGGC dans le but de prévenir, détecter et gérer les cyberattaques et autres incidents de sécurité.

(149) L'entrepreneur doit également fournir un COSI de secours qui, sans être situé physiquement dans les mêmes installations (c'est-à-dire même immeuble) que le centre principal des opérations, offre toutes les fonctionnalités opérationnelles et de gestion prises en charge par ce centre.

(150) La transition du COSI principal vers le COSI de secours doit se faire de façon transparente pour le Canada et ne doit pas avoir d'incidence sur les opérations du SSGGC.

(151) L'entrepreneur doit effectuer la transition du COSI principal vers le COSI de secours, conformément au plan de continuité du service.

(152) L'entrepreneur doit mettre à l'essai chaque année la transition du COSI principal vers le COSI de secours et fournir au Canada un rapport contenant les résultats des essais et les recommandations pertinentes.

(153) Le COSI doit surveiller les incidents de sécurité en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année).

(154) L'entrepreneur doit fournir les composantes matérielles et logicielles nécessaires à la surveillance, à la compilation, à l'analyse et à la déclaration des incidents de sécurité.

(155) Le COSI doit être certifié ISO 27001.

(156) L'entrepreneur doit résoudre les incidents de sécurité en collaboration avec le Centre de protection de l'information du Canada et toute autre partie que celui-ci désigne en appliquant un processus mutuellement convenu entre le Canada et l'entrepreneur.

(157) L'entrepreneur doit notifier le Canada, par téléphone ou par courriel en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année), de tout incident de sécurité présumé ou réel, y compris sans s'y limiter les intrusions non autorisées, les attaques par déni de service, les cas de fraude détectés et autres atteintes à la sécurité visant son centre des opérations ou son COSI.

(158) Lors d'un incident de sécurité, l'entrepreneur doit réduire le temps de réponse standard dans ses services de gestion selon la gravité de l'incident de sécurité, tel que le définit le Canada.

(159) En plus de toute autre source de renseignements sur les cybermenaces et les incidents qu'il surveille dans le cadre de ses activités courantes, l'entrepreneur doit également surveiller les publications de cybermenaces et d'incidents qui proviennent de sources recensées par le Canada (p. ex. le Centre canadien de réponse aux incidents cybernétiques [http://www.publicsafety.gc.ca/prg/em/ccirc/anre-fra.aspx]). Cette surveillance doit être effectuée en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année) et corriger en priorité les vulnérabilités relevées dans les publications qui ont une incidence sur toute composante intervenant dans la prestation du SSGGC au Canada, selon leur criticité, et ce, sans frais supplémentaires pour le Canada.

3.3 Continuité du service

(160) L'entrepreneur doit mettre en œuvre et tester le plan de continuité du service (l'ensemble des processus, procédures, rôles, responsabilités, etc.) dans les 60 JOFPF suivant l'acceptation du SSGGC par le Canada, et fournir les résultats du test au Canada dans les 10 JOFPF en suivant la réalisation.

(161) L'entrepreneur doit corriger tout problème décelé au cours de la mise à l'essai du plan de continuité du service.

(162) L'entrepreneur doit fournir au Canada, dans les 40 JOFPF suivant une demande, la preuve que le plan de continuité du service a été convenablement mis en œuvre, qu'il fonctionne comme prévu et qu'il produit les résultats escomptés. La preuve peut prendre la forme de résultats de tests, d'évaluations, de vérifications ou autres, et ne peut dater de plus de 24 mois.

(163) L'entrepreneur doit fournir au Canada, dans les 30 JOFPF suivant chaque date anniversaire du contrat, une mise à jour de son plan de continuité du service.

3.4 Centre de services

(164) L'entrepreneur doit fournir un centre de services que les représentants autorisés des ministères pourront joindre en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année) pour obtenir de l'aide.

(165) Le centre de services doit authentifier l'identité du demandeur.

(166) Le centre de services doit accepter les courriels que les représentants autorisés des ministères du Canada envoient à la boîte aux lettres électronique fournie par

l'entrepreneur. Cette boîte aux lettres doit être dotée d'une fonction de réponse automatique pour accuser réception du courriel.

(167) Le centre de services doit accuser réception des courriels provenant d'adresses de courriel autorisées par le Canada dans les 15 minutes suivant leur réception, et ce, en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année).

(168) L'entrepreneur doit fournir, à l'égard du centre de services, les numéros de téléphone qui suivent, ainsi que les services connexes liés au réseau téléphonique public commuté :

a) Les numéros d'appel sans frais pour l'Amérique du Nord;

b) Les numéros d'accès au service TTY/ATS (téléimprimeur/appareil de télécommunication pour personnes sourdes);

c) Le numéro d'appel local pour la RCN.

(169) Le centre de services doit répondre aux appels (en personne ou par message préenregistré) dans l'une des deux langues officielles (français ou anglais) du Canada, selon la langue qu'a choisie l'appelant en réponse au message qui lui a été communiqué au départ dans les deux langues.

(170) Le centre de services doit rediriger (transférer) les appels au spécialiste des opérations et des mesures d'intervention de sécurité lorsqu'un représentant autorisé du Canada en fait la demande, en appliquant le transfert d'appel assisté, et ce, dans les cinq minutes.

(171) Le centre de services doit permettre aux représentants autorisés du Canada d'éviter la liste d'attente et de joindre immédiatement un de ses agents.

4 SERVICES DE GESTION

(172) L'entrepreneur doit fournir l'ensemble des logiciels et du matériel nécessaire pour exécuter les services de gestion du SSGGC.

(173) L'entrepreneur doit fournir les services de gestion à l'égard du SSGGC sans que le Canada ait à engager des frais additionnels à cet égard.

(174) L'entrepreneur doit utiliser une connexion sécurisée (chiffrée) et fiable, prévoyant entre autres une authentification forte de l'utilisateur, la non-répudiation des modifications et la protection de l'intégrité des données, pour assurer l'administration et la gestion à distance des services gérés du SSGGC, en appliquant un processus approuvé par le Canada.

(175) L'administration et la gestion à distance ne doivent pas dépendre uniquement de la connectivité dans la bande.

(176) Le SSGGC doit enregistrer les communications liées à la gestion à distance et fournir les registres des activités au Canada dans les cinq JOFPF suivant la demande présentée par celui-ci à cet effet.

(177) L'entrepreneur doit offrir les services de gestion suivants pour le SSGGC en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année) :

a) La gestion des changements (voir la sous-section Gestion des changements);

b) La gestion de la configuration (voir la sous-section Gestion de la configuration);

c) La gestion des incidents (voir la sous-section Gestion des incidents);

d) La gestion des mises en production (voir la sous-section Gestion des mises en production);

e) La gestion de la capacité (voir la sous-section Gestion de la capacité);

f) La gestion de la disponibilité (voir la sous-section Gestion de la disponibilité).

4.1 Gestion des changements

(178) L'entrepreneur doit créer une demande de changement pour tous les changements apportés au matériel, aux logiciels, aux applications et aux processus qu'il utilise pour livrer le SSGGC, et soumettre cette demande au Canada.

(179) Toutes les demandes de changement doivent être approuvées par le Canada, sauf dans le cas des changements d'urgence.

(180) Les changements apportés au réseau et à l'infrastructure du système de soutien de l'entrepreneur qui ne sont pas reliés aux services du SSGGC livrés au Canada ne nécessitent pas l'approbation du Canada.

(181) Le Canada fournira à l'entrepreneur la liste de personnes autorisées à approuver les demandes de changement.

(182) L'entrepreneur doit créer au moins un billet de changement pour chaque demande de changement présentée par le Canada, et ce, dans un JOFPF suivant la réception de la demande de changement.

(183) L'entrepreneur doit accepter en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année) les demandes de changement que lui transmet le Canada par courriel à une boîte aux lettres électronique qu'il fournit; cette boîte aux lettres doit être dotée d'une fonction de réponse automatique de façon à accuser réception du courriel.

(184) L'entrepreneur doit donner suite aux demandes de changement, à l'exception des changements d'urgence, pendant les périodes de maintenance approuvées par le Canada.

(185) L'entrepreneur doit assigner les demandes de changements selon leur priorité de mise en œuvre établie en fonction des niveaux de priorité précisés par le Canada.

(186) L'entrepreneur doit classer les demandes de changement présentant une incidence en fonction de l'échelle approuvée par le Canada à cet effet, et les assigner en conséquence.

(187) L'entrepreneur doit revoir l'incidence que comporte une demande de changement lorsque le Canada lui demande de le faire, et ce, dans l'heure suivant la demande.

(188) L'entrepreneur doit signaler les demandes de changement aux paliers d'intervention supérieurs selon leur type et leur gravité, et la période pendant laquelle elles sont restées ouvertes.

(189) L'entrepreneur doit fournir au Canada une matrice de signalisation aux paliers d'intervention supérieurs de la gestion et des opérations; cette matrice dressera la liste du personnel, ainsi que des suppléants (de même autorité hiérarchique), pour chaque palier d'intervention et fournira des instructions claires sur la procédure de communication.

(190) L'entrepreneur doit aviser le Canada d'une demande de changement, selon la matrice de signalisation aux paliers d'intervention supérieurs de la gestion et des opérations.

(191) L'entrepreneur doit signaler les demandes de changement à la demande du Canada.

(192) Le billet de changement doit comprendre, sans s'y limiter, les zones d'information dédiées suivantes pour toutes les demandes de changement, et l'entrepreneur doit maintenir l'information à jour :

a) Numéro de billet;

b) Description du changement;

c) Billets de changement connexes;

d) Estampille temporelle indiquant la date et l'heure d'ouverture du billet;

e) Estampille temporelle indiquant la date et l'heure de fermeture du billet;

f) Type;

g) Impact sur le client;

h) Fonctions touchées (ouverture de session, enregistrement, établissement de billets, établissement de rapports, surveillance, etc.);

i) État (ouvert, fermé, en cours, approuvé, en suspens, annulé, infructueux, échec, etc.);

j) Numéro du billet de changement du Canada;

k) Information sur les personnes-ressources de l'entrepreneur (nom, numéro de téléphone et adresse de courriel);

l) Identificateur du client;

m) Information sur les personnes-ressources du Canada (nom, numéro de téléphone et adresse de courriel);

n) Registre des activités, y compris de l'ensemble des mesures prises par les tiers;

o) Date et heure prévues du changement;

p) Date et heure prévues de l'exécution du changement;

q) Nom des approbateurs du changement;

r) Plan de test d'acceptation;

s) Procédures d'annulation (retour arrière);

t) Billets d'incident connexes.

(193) L'entrepreneur doit revoir le contenu des zones d'information des billets de changement ou du plan de test d'acceptation des changements, à la demande du Canada.

(194) L'entrepreneur doit mettre à jour le journal d'information sur les billets de changement à la suite d'un changement d'état fondé sur le niveau de gravité, selon ce que précise le Canada.

(195) L'entrepreneur doit automatiquement mettre à jour l'état d'un billet de changement dans les 30 minutes suivant un changement dans l'état du billet, comme en fait foi l'estampille temporelle.

(196) L'entrepreneur doit mettre à jour l'état d'un billet de changement (échec, infructueux, réussi, etc.), tel que le précise le Canada, en fonction des tests d'acceptation relatifs aux changements et des résultats de la procédure d'annulation (si elle a été mise en œuvre).

(197) L'entrepreneur doit transmettre par courriel à une liste de distribution prédéfinie déterminée par le Canada l'information concernant le billet de changement, dans le cas de demandes de changement précisées par le Canada, jusqu'à ce que les billets de changement liés à ces demandes soient fermés ou que le Canada annule la déclaration automatique des mises à jour, en fonction des changements d'état des billets.

(198) L'entrepreneur doit annuler les changements, lorsque le Canada en fait la demande, à l'aide des procédures d'annulation précisées dans le billet de changement, lesquelles prévoient entre autres :

a) Les tâches et activités à exécuter pour ramener le service (fonctionnalité et données) à son état antérieur au changement;

b) Les résultats opérationnels prévus suite à l'exécution de la procédure d'annulation;

c) Les critères à appliquer pour vérifier si l'annulation a réussi;

d) L'enregistrement, dans le registre des activités du billet de changement, des résultats de la procédure d'annulation.

(199) L'entrepreneur doit annuler les changements lorsque les critères d'acceptation précisés à l'égard d'une demande de changement n'ont pas été satisfaits après mise en œuvre, en appliquant les procédures d'annulation mentionnées dans le billet de changement.

(200) L'entrepreneur doit transmettre au Canada un avis de mise en œuvre de la demande de changement dans les 48 heures au plus tard précédant la mise en œuvre de la demande, lorsqu'il a évalué, approuvé et fait tous les préparatifs nécessaires pour mettre en œuvre ladite demande.

(201) L'entrepreneur dot transmettre au Canada un avis d'annulation de la demande de changement dans les 24 heures suivant l'annulation, par lui-même, de ladite demande.

(202) L'entrepreneur doit effectuer des tests d'acceptation du changement en appliquant le plan de test d'acceptation, précisé dans le billet de changement et approuvé par le Canada, et rendre compte des résultats des tests dans le registre des activités du billet de changement.

(203) L'entrepreneur doit consigner les résultats du test d'acceptation dans le billet de changement, dans les deux JOFPF suivant l'exécution d'une demande de changement.

(204) L'entrepreneur doit exécuter avec succès le plan de test d'acceptation figurant dans le billet de changement, avant que le Canada accepte la demande de changement.

(205) L'entrepreneur doit fermer les billets de changement liés à une demande de changement après que la demande a été acceptée par le Canada.

(206) L'entrepreneur doit fournir au Canada un avis d'exécution de la demande de changement dans les deux JOFPF suivant l'exécution de la demande de changement.

(207) L'entrepreneur doit permettre au Canada d'accéder aux billets de changement au moyen du portail de services, qui prévoit notamment ce qui suit :

a) La recherche et le tri des billets de changement ouverts et fermés selon la zone d'information du billet que choisit le Canada à l'égard d'une période de déclaration (date de début ou de fin) et d'un intervalle (année, mois, jour, heure);

b) Le téléchargement des résultats de la recherche visant les billets de changement en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada;

c) La visualisation des billets de changement dans une structure hiérarchique dans le cadre de laquelle il est possible de visualiser un billet (c'est-à-dire un billet connexe) par forage descendant;

d) La visualisation de l'information sommaire concernant les billets de changement ouverts ou fermés, présentée sous forme de tableau ou de graphique par année, mois, jour et heure selon une période sélectionnée par le Canada pour certains billets triés par type, niveau de gravité et état.

4.2 Gestion de la configuration

(208) La gestion de la configuration que réalise l'entrepreneur à l'égard du SSGGC doit comprendre ce qui suit :

a) La configuration et la programmation de toutes les fonctions, caractéristiques et modifications touchant les composantes matérielles et logicielles, afin que les exigences opérationnelles continues du SSGGC soient conformes aux exigences du Canada;

b) La mise en œuvre des correctifs matériels et logiciels;

c) Le maintien à jour de l'information concernant les configurations et de l'état de toutes les composantes matérielles et logicielles;

d) La sauvegarde quotidienne des fichiers de configuration et des changements qui y sont apportés, et le maintien des fichiers de configuration de sauvegarde dans un emplacement hors site;

e) Le maintien à jour des fichiers journaux de configuration qui comprendront une entrée pour chaque changement apporté à la configuration; chaque entrée doit contenir ce qui suit :

i) La date et l'heure du changement;

ii) Le nom de la ressource apportant le changement;

f) L'archivage des fichiers journaux de configuration pendant une période de trois ans;

g) La publication, dans un format de fichier commercial approuvé par le Canada, de l'information sur la configuration de chaque composante matérielle et logicielle figurant sur le portail de services et la mise à jour de l'information publiée en fonction des niveaux de priorité précisés par le Canada;

h) Le maintien à jour de l'information courante concernant la configuration ainsi que le maintien de deux copies antérieures de cette information;

i) Le suivi de l'état d'un élément de configuration à mesure qu'il passe d'un état à un autre, par exemple « en cours d'élaboration », « à l'essai », « mis en service » ou « retiré »).

(209) L'entrepreneur doit créer et tenir à jour des graphiques concernant le SSGGC et les fournir au Canada dans les cinq JOFPF suivant une demande; ces graphiques indiqueront ce qui suit :

a) La connectivité physique et logique de toutes les composantes du SSGGC;

b) La classification du trafic;

c) L'attribution des adresses IP.

(210) L'entrepreneur doit fournir l'information sur la configuration des composantes matérielles et logicielles lorsque le Canada lui en fait la demande, en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada, en fonction des niveaux de priorité précisés par le Canada.

(211) L'entrepreneur doit déménager le SSGGC d'un PPS vers un autre PPS précisé par le Canada, dans les 20 JOFPF suivant une demande écrite (présentée par courriel) par le Canada.

(212) L'entrepreneur doit retirer le SSGGC d'un PPS précisé par le Canada, dans les 20 JOFPF suivant une demande écrite (présentée par courriel) par le Canada.

(213) L'entrepreneur doit mettre sous tension et mettre hors tension le SSGGC, à un PPS déterminé par le Canada et selon un calendrier de maintenance qu'il précise, dans les 60 JOFPF suivant une demande écrite (présentée par courriel) par le Canada.

(214) L'entrepreneur doit, dans les trois mois suivant leur accessibilité générale, installer des versions commerciales de maintenance de logiciels publiées par le fabricant d'équipement d'origine pour le matériel et le logiciel fournis par l'entrepreneur pour le SSGGC, sans coûts additionnels pour le Canada.

4.3 Gestion des incidents

(215) L'entrepreneur doit résoudre les incidents.

(216) L'entrepreneur doit résoudre les incidents en collaboration avec le Canada et toute autre partie que celui-ci désigne en appliquant un processus mutuellement convenu entre le Canada et l'entrepreneur.

(217) L'entrepreneur doit classer les incidents en fonction de leur gravité et en prioriser la résolution conformément aux niveaux de gravité et de priorisation des incidents déterminés par le Canada, et les assigner en conséquence.

(218) L'entrepreneur doit consigner comme incident toutes les atteintes à la vie privée ou infractions à la sécurité, et autres événements liés à la sécurité.

(219) L'entrepreneur doit revoir le niveau de gravité d'un incident lorsque le Canada lui demande de le faire, dans les cinq minutes suivant la demande.

(220) L'entrepreneur doit signaler les incidents aux paliers d'intervention supérieurs en fonction de leur type, gravité, priorisation et de la période pendant laquelle le billet est resté ouvert.

(221) L'entrepreneur doit fournir au Canada une matrice de signalisation aux paliers d'intervention supérieurs de la gestion et des opérations dans les cinq JOFPF suivant une demande présentée par le Canada; cette matrice dressera la liste du personnel ainsi que des suppléants (de même autorité hiérarchique) pour cinq paliers d'intervention au minimum (du 1er au 5^{e} palier d'intervention, le 5^{e} palier regroupant le personnel du niveau hiérarchique le plus élevé) et fournira des instructions claires sur la procédure de communication.

(222) L'entrepreneur doit aviser le Canada des incidents, selon la matrice de signalisation aux paliers d'intervention supérieurs de la gestion et des opérations et en fonction de leur niveau de gravité, comme le précise le Canada.

(223) L'entrepreneur doit changer le palier d'intervention à l'égard des incidents lorsque le Canada lui en fait la demande, et ce, en fonction des niveaux de priorité qu'il précise.

(224) L'entrepreneur doit signaler les incidents au personnel de chaque palier d'intervention selon le niveau de gravité dans le délai précisé par le Canada (c'est-à-dire signalisation des incidents de gravité 2 au personnel du 1er palier d'intervention dans les deux heures suivant l'établissement du billet d'incident).

(225) L'entrepreneur doit créer au moins un billet d'incident pour chaque incident.

(226) L'entrepreneur doit automatiquement transmettre par courriel à une liste de distribution prédéfinie déterminée par le Canada l'information concernant le billet d'incident, dans le cas d'incidents précisés par le Canada, jusqu'à ce que le billet d'incident soit fermé ou que le Canada annule la déclaration automatique des mises à jour, en fonction des changements d'état du billet.

(227) Le billet d'incident doit comprendre, sans s'y limiter, les zones d'information dédiées suivantes pour tous les incidents, et l'entrepreneur doit maintenir l'information à jour :

a) Numéro de billet;

b) Description de l'incident;

c) Entité ayant signalé l'incident (entrepreneur, représentant du Canada);

d) Billets d'incident connexes;

e) Billets de changement connexes;

f) Estampille temporelle indiquant la date et l'heure d'ouverture du billet d'incident;

g) Estampille temporelle indiquant la date et l'heure de fermeture du billet d'incident;

h) Type d'incident (production, test fonctionnel, test de performance, sécurité, etc.), selon ce que précise le Canada;

i) Gravité de l'incident;

j) État (ouvert, fermé, en cours, approuvé, en suspens, annulé, etc.);

k) Numéro du billet du Canada;

l) Fonctions du service touchées;

m) Nom de la personne-ressource du centre de services à contacter pour établir le billet (nom, numéro de téléphone et adresse de courriel);

n) Information sur les personnes-ressources de l'entrepreneur (nom, numéro de téléphone et adresse de courriel);

o) Identificateur de l'organisation cliente ou de l'utilisateur (selon ce que précise le Canada);

p) Type d'organisation cliente ou d'utilisateur (selon ce que précise le Canada);

q) Langue associée à l'organisation cliente ou langue de l'utilisateur;

r) Information sur les personnes-ressources du ministère (nom, numéro de téléphone et adresse de courriel);

s) Registre des activités, y compris de l'ensemble des mesures prises par les tiers;

t) Description des mesures de résolution et cause;

u) Temps d'interruption (billets fermés seulement);

v) Estampille temporelle indiquant la date et l'heure de la dernière mise à jour du billet;

w) Fichiers joints.

(228) L'entrepreneur doit ouvrir un billet d'incident dans les cinq minutes suivant la détermination de l'incident par l'entrepreneur et son signalement par le Canada.

(229) L'entrepreneur doit mettre à jour le journal d'information sur les billets d'incident à la suite d'un changement d'état fondé sur le niveau de gravité, selon ce que précise le Canada.

(230) L'entrepreneur doit documenter toutes les signalisations d'incidents aux paliers d'intervention supérieurs techniques ou de la gestion dans le journal d'information sur les billets d'incident.

(231) L'entrepreneur doit documenter, dans le journal d'information sur les billets d'incident, toutes les interactions qu'il a avec des tiers au sujet des incidents.

(232) L'entrepreneur doit tenir compte du temps d'interruption lié à chaque incident et le signaler dans le billet d'accident connexe.

(233) Le temps d'interruption lié à un incident doit commencer au moment où l'entrepreneur détecte l'incident ou au moment où le Canada le signale à l'entrepreneur.

(234) Le temps d'interruption lié à un incident doit prendre fin au moment où le SSGGC est complètement rétabli, à la suite de cet incident, et où le Canada approuve la fermeture du billet d'incident connexe.

(235) L'entrepreneur doit suspendre la résolution d'un incident (en plaçant le compteur de temps d'interruption en mode attente) à la demande du Canada.

(236) La résolution d'un incident suspendue par le Canada demeure en suspens tant que celui-ci n'en a pas autorisé la reprise ou pendant une période déterminée qu'il précise.

(237) L'entrepreneur ne doit pas suspendre la résolution d'un incident sans avoir obtenu l'approbation du Canada, sauf dans le cas où le Canada ne peut fournir, à la demande de l'entrepreneur, l'information nécessaire s'y rapportant.

(238) L'entrepreneur doit reprendre la résolution (redémarrage du compteur de temps d'interruption à compter du moment de la suspension) d'un incident qu'il a suspendue lorsque le Canada lui communique l'information demandée.

(239) L'entrepreneur doit suspendre la période d'interruption liée à un incident à la demande du Canada ou lorsqu'il demande la fermeture d'un billet d'incident pendant qu'il attend l'approbation du Canada et que celui-ci ne peut examiner sa demande, pour cause d'indisponibilité.

(240) L'entrepreneur doit redémarrer la période d'interruption suspendue lorsque le Canada en fait la demande ou que, après examen de la demande de fermeture du billet d'incident, il détermine que le billet doit rester ouvert.

(241) L'entrepreneur doit obtenir l'approbation du Canada avant de fermer les billets d'incident.

(242) L'entrepreneur doit fermer le billet d'incident après que le Canada en a approuvé la fermeture.

(243) L'entrepreneur doit aviser le Canada de la résolution d'un incident selon le niveau de gravité précisé par le Canada.

(244) Si un billet d'incident est fermé et qu'un nouvel incident survient dans les 24 heures à cause du même problème, l'entrepreneur doit rouvrir le billet d'incident initial ou ouvrir

un nouveau billet qui renverra à l'incident précédent, et signaler le moment de l'ouverture par rapport au billet initial.

(245) L'entrepreneur doit déterminer et documenter les facteurs déterminants (causes fondamentales) de tous les incidents.

(246) L'entrepreneur doit concevoir des solutions de rechange pour s'attaquer à toutes les causes fondamentales décelées.

(247) L'entrepreneur doit qualifier de problème chronique tout incident qui se produit trois fois ou plus dans une période de 90 jours consécutifs et dont la cause fondamentale est la même.

(248) L'entrepreneur doit assigner le niveau de gravité le plus élevé suivant aux incidents qualifiés de problèmes chroniques.

(249) L'entrepreneur doit relier les incidents aux problèmes chroniques existants ou nouveaux, à la demande du Canada.

(250) L'entrepreneur doit permettre au Canada d'accéder aux billets d'incident au moyen du portail de services, qui prévoit notamment ce qui suit :

a) La recherche et le tri des billets d'incident ouverts et fermés selon la zone d'information du billet que choisit le Canada à l'égard d'une période de déclaration (date de début ou de fin) et d'un intervalle (année, mois, jour, heure);

b) Le téléchargement des résultats de la recherche visant les billets d'incident en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada;

c) La visualisation des billets d'incident dans une structure hiérarchique dans le cadre de laquelle il est possible de visualiser un billet (c'est-à-dire un billet connexe) par forage descendant;

d) La visualisation de l'information sommaire concernant les billets d'incident ouverts ou fermés, présentée sous forme de tableau ou de graphique par année, mois, jour et heure selon une période sélectionnée par le Canada pour certains billets triés par type, niveau de gravité et état.

4.3.1 Gestion des incidents de sécurité

(251) L'entrepreneur doit notifier le Canada, par téléphone et par courriel en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année), de tout incident de sécurité présumé ou réel, y compris les intrusions non autorisées, les attaques par déni de service, les cas de fraude détectés et autres atteintes à la sécurité.

(252) L'entrepreneur doit commencer les procédures d'intervention en cas d'incident de sécurité, en fonction des niveaux de priorité précisés par le Canada.

(253) Le billet d'incident lié aux incidents de sécurité doit contenir, sans s'y limiter, les renseignements suivants :

a) Le type et la description de l'attaque, de l'incident ou de l'événement;

b) Des éléments d'information pouvant indiquer si l'attaque semble avoir réussi et l'impact de celle-ci, le cas échéant;

c) La portée de l'attaque (pour une ou plusieurs organisations clientes);

d) L'estimation du nombre de systèmes touchés, par organisation cliente;

e) La liste des systèmes d'extrémité touchés, par organisation cliente;

f) La source ou provenance apparente de l'attaque, de l'incident ou de l'événement;

g) Les mesures prises;

h) L'état d'avancement des mesures d'atténuation;

i) Les registres ou données probantes applicables.

(254) L'entrepreneur doit mettre en œuvre les mesures d'atténuation (p. ex. blocage de pare-feu, filtrage d'URL, signatures d'intrusion personnalisées) pour confiner un incident de sécurité, lorsque les représentants autorisés du Canada en font la demande, selon ce que précise le Canada conformément au niveau de priorité qu'il détermine.

(255) L'entrepreneur doit établir une demande de changement d'urgence, selon la gravité précisée par le Canada, à l'égard de chaque mesure d'atténuation que demande le Canada en vue du confinement d'un incident de sécurité, et exécuter cette demande en fonction des niveaux de priorité que précise celui-ci.

(256) L'entrepreneur doit chiffrer, à l'aide d'une méthode de chiffrement approuvée par le Canada, l'information concernant l'incident de sécurité qui est transmise autrement que par l'entremise du portail de services.

4.4 Gestion des mises en production

(257) La gestion des mises en production doit comprendre :

a) L'intégration avec les processus de gestion des changements, de gestion des incidents et de gestion de la configuration;

b) La planification, la mise à l'essai et le déploiement de composantes matérielles et logicielles nouvelles et modifiées;

c) Un plan ou un calendrier de mises en production sur une période consécutive de 12 mois;

d) L'élaboration et la mise en œuvre de procédures visant la répartition et l'installation des changements, ainsi que le retour arrière;

e) La coordination des communications relatives aux versions logicielles;

f) La distribution des logiciels.

(258) L'entrepreneur doit fournir les notes relatives à la mise en production pour toute mise en production du SSGGC au moins 40 JOFPF avant sa mise en œuvre.

(259) L'entrepreneur ne doit mettre en œuvre aucune mise en production du SSGGC avant d'avoir obtenu l'approbation du Canada.

(260) L'entrepreneur doit participer aux réunions portant sur l'examen de la gestion des mises en production; ces réunions sont organisées par le Canada dans la RCN pour discuter des mises en production du SSGGC à venir, tel que le demande le Canada.

(261) L'entrepreneur doit fournir, dans les 30 jours suivant la demande présentée par le Canada, un plan annuel à jour de mise en production. Le plan annuel de mise en production comprendra un calendrier et indiquera les fonctionnalités et particularités techniques de tout changement prévu au service qu'il fournit. Le plan annuel de mise en production doit prévoir des périodes de test pour le Canada.

4.5 Gestion de la capacité

(262) La gestion de la capacité à l'égard du SSGGC doit comprendre :

a) L'examen et l'analyse des statistiques concernant la performance du service, de même que des niveaux de service, afin de cerner les lacunes ou problèmes ayant trait à la capacité;

b) L'analyse de l'incidence des nouvelles mises en production sur la capacité du service;

c) L'adaptation, la mise au point et l'amélioration des services afin d'assurer une utilisation et une performance optimales;

d) Le plan de gestion de la capacité et les prévisions connexes;

e) L'évaluation des exigences du Canada en matière de capacité et la formulation de recommandations à l'égard des changements à apporter aux services sur le plan de la capacité.

4.6 Gestion de la disponibilité

(263) La gestion de la disponibilité doit comprendre :

a) L'examen des exigences en matière de disponibilité et l'assurance que les plans d'urgence sont mis en place et testés régulièrement pour garantir que les exigences de prestation des services sont satisfaites;

b) La détermination proactive de problèmes de disponibilité afin qu'ils puissent être résolus avant d'avoir un impact sur les utilisateurs;

c) L'analyse des données concernant la disponibilité afin de cerner les problèmes de disponibilité;

d) La configuration des services pour assurer la disponibilité prévue au contrat.

(264) L'entrepreneur doit signaler au Canada, dans le cadre de réunions hebdomadaires portant sur l'examen opérationnel, les problèmes qui pourraient avoir une incidence sur la disponibilité ou occasionner des lacunes sur le plan de la capacité, y compris la proposition de solutions pour assurer la disponibilité prévue au contrat.

(265) L'entrepreneur doit notifier le Canada des interruptions planifiées du SSGGC au moins 20 JOFPF à l'avance.

(266) L'entrepreneur ne doit pas prévoir plus de deux périodes d'interruption planifiées de quatre heures du SSGGC à un PPS par année civile.

(267) L'entrepreneur doit obtenir l'approbation du Canada pour toute interruption planifiée du SSGGC.

5 RÉUNIONS

(268) Les réunions doivent se tenir pendant les heures de bureau (entre 8 h et 17 h HE) les JOFPF dans la RCN et en personne, à moins d'indication contraire dans l'Énoncé des travaux ou selon ce que précise le Canada.

(269) Le Canada peut organiser une réunion visant l'examen et la planification du contrat; cette réunion se tiendra tous les trimestres. L'entrepreneur doit assister à cette réunion à la demande du Canada.

(270) Cette réunion prévoira un examen des points suivants, liés aux travaux à accomplir :

a) Le rendement au chapitre de la gestion du service pour le trimestre précédent;

b) Les problèmes importants touchant la prestation des services et le soutien du service survenus au cours du trimestre précédent;

c) Les améliorations importantes prévues au chapitre de la prestation des services et du soutien du service au cours du trimestre à venir;

d) Les risques, possibilités et objectifs pour le trimestre à venir.

(271) L'entrepreneur doit organiser des réunions hebdomadaires portant sur l'examen opérationnel et y participer par téléconférence ou d'autres moyens précisés par le Canada. Ces réunions visent à examiner les incidents ayant une incidence sur la prestation des services et le résultat des changements apportés depuis la dernière réunion.

(272) L'entrepreneur doit organiser des réunions mensuelles portant sur l'examen opérationnel et y participer par téléconférence ou d'autres moyens précisés par le Canada. Ces réunions ont pour objet de passer en revue les problèmes qui se sont produits depuis la dernière réunion mensuelle, l'état d'avancement des interventions en cours à l'égard des problèmes et l'approbation et la planification des mesures correctives recommandées dans les rapports d'ACF.

(273) L'entrepreneur doit organiser, à la demande du Canada, des réunions portant sur la gestion des changements et y participer par téléconférence ou d'autres moyens précisés par le Canada. Ces réunions visent à examiner les résultats des demandes de changement exécutées la semaine précédente, les demandes de changement prévues pour la prochaine semaine et celles soumises par l'entrepreneur pour approbation par le Canada.

(274) L'entrepreneur doit organiser tous les six mois une réunion portant sur l'examen de la gestion des niveaux de service et y participer par téléconférence ou d'autres moyens précisés par le Canada. Cette réunion portera sur l'examen des données relatives à l'atteinte des niveaux de service au cours des six mois précédents. Pour cette réunion, l'entrepreneur doit être prêt à discuter de tout manquement à cet égard, à décrire les mesures prises pour prévenir la répétition des événements touchant le service et à discuter des plans d'évolution du service pour les six prochains mois.

6 RAPPORTS ET DOCUMENTS

(275) L'entrepreneur doit fournir tous les documents portant sur le SSGGC en anglais et dans un format de fichier commercial approuvé par le Canada.

(276) L'entrepreneur doit fournir tous les rapports portant sur le SSGGC en anglais et dans un format de fichier commercial approuvé par le Canada.

(277) Tous les documents et rapports portant sur le SSGGC et fournis par l'entrepreneur doivent être accessibles au moyen du portail de services, à moins d'avis contraire du Canada.

(278) L'entrepreneur doit assurer le suivi des versions et tenir un historique des modifications à l'égard des changements apportés aux documents et rapports portant sur le SSGGC.

(279) L'entrepreneur doit archiver les données se rapportant à tous les rapports concernant le SSGGC pendant la durée du contrat et, sur demande écrite du Canada, fournir à

celui-ci, dans les 20 JOFPF, les renseignements demandés dans un fichier, suivant le format et les règles régissant le nom des fichiers qu'il précise.

(280) À moins d'indication contraire concernant un rapport précis mentionné dans l'Énoncé des travaux, l'entrepreneur doit fournir les rapports mensuels au plus tard cinq JOFPF suivant le mois précédent visé par le rapport, les rapports hebdomadaires au plus tard le deuxième JOFPF suivant la semaine précédente visée par le rapport, les rapports quotidiens au plus tard à 9 h HE le prochain JOFPF et les rapports spéciaux dans les cinq JOFPF suivant une demande présentée par le Canada.

(281) L'entrepreneur doit mettre à jour les diagrammes et documents concernant le SSGGC à la suite d'un changement qui, selon le cas :

a) A une incidence sur les renseignements qu'ils contiennent;

b) Est exigé par le Canada pour leur acceptation.

6.1 Rapports mensuels

(282) L'entrepreneur doit fournir un rapport mensuel sur les activités de mise en œuvre du plan de traitement des risques.

(283) L'entrepreneur doit fournir au Canada un rapport mensuel sur l'évolution du contrat en ce qui concerne notamment :

a) Les réalisations et plans;

b) Les problèmes liés aux niveaux de service et nécessitant une résolution;

c) Les risques, y compris les probabilités s'y rapportant et les mesures d'atténuation;

d) Les problèmes nécessitant une résolution;

e) Les litiges concernant la facturation et nécessitant une résolution.

(284) L'entrepreneur doit fournir au Canada un rapport mensuel présenté sous forme de tableau ou de graphique qui indique, pour chaque niveau de service ainsi que par organisation cliente :

a) Le PPS;

b) La plateforme de service;

c) Les services de sécurité du SSGGC livrés par la plateforme de service;

d) Les données concernant l'ensemble des niveaux de service pour les 60 derniers jours, ventilées par jour, y compris une représentation du profil horaire pendant cette période;

e) Les données concernant l'ensemble des niveaux de service pour les 13 derniers mois, ventilées par jour;

f) Les données concernant l'ensemble des niveaux de service depuis l'adjudication du contrat, ventilées par mois, y compris une représentation du profil horaire pour chaque mois, le cas échéant.

(285) L'entrepreneur doit fournir au Canada, pour chaque organisation cliente, un rapport mensuel présenté sous forme de tableau ou de graphique qui indique, pour chaque occurrence où le niveau de service n'a pas été atteint :

a) Le PPS;

b) La plateforme de service;

c) Les services de sécurité du SSGGC livrés par la plateforme de service;

d) Le niveau de service calculé;

e) Le niveau de service prévu au contrat;

f) Une description des circonstances expliquant l'incapacité à respecter un niveau de service donné;

g) Les crédits de service applicables.

(286) L'entrepreneur doit fournir au Canada un rapport mensuel portant sur les problèmes chroniques qui comprend ce qui suit :

a) La description des problèmes chroniques;

b) Les mesures prises pour les résoudre;

c) Les recommandations sur la marche à suivre pour que de tels problèmes ne se reproduisent pas à l'avenir.

(287) L'entrepreneur doit fournir au Canada un rapport de gestion mensuel sur l'état des opérations comprenant ce qui suit, par organisation cliente :

a) Un résumé;

b) Un rapport sous forme de tableau ou de graphique illustrant sur une période de 13 mois :

i) Les valeurs cibles et réelles, et le nombre d'exceptions pour chaque niveau de service;

ii) Le nombre de demandes de changement présentées, échouées, en suspens et exécutées;

iii) Le temps minimal, maximal et moyen écoulé entre les délais de mise en œuvre planifiés et réels pour exécuter les demandes de changement;

iv) Le nombre de billets d'incident ouverts, fermés et en suspens;

v) Le temps minimal, maximal et moyen écoulé pour ouvrir et fermer un billet d'incident, selon le niveau de gravité et le type d'incident;

c) Un résumé des incidents de sécurité et des mesures prises;

d) Un résumé des demandes de changement d'urgence;

e) Les détails concernant les incidents et les demandes de changement comportant un indicateur visant à signaler les situations où le processus de signalisation a échoué ou n'a pas été suivi;

f) Une description des mesures correctives et des délais pour mettre en œuvre les changements nécessaires visant à prévenir des défaillances futures à l'égard des niveaux de service.

(288) L'entrepreneur doit fournir au Canada un rapport mensuel indiquant ce qui suit pour chaque capacité de gestion des menaces du SSGGC, sur le plan de la performance :

a) Le nom de l'organisation cliente;

b) Le PPS;

c) La plateforme de service;

d) Les services de gestion des menaces offerts par la plateforme de service;

e) La date et l'heure du début;

f) La date et l'heure de la fin;

g) L'utilisation moyenne et maximale de la mémoire;

h) L'utilisation moyenne et maximale du processeur;

i) L'utilisation moyenne et maximale de la bande passante;

j) La date du dernier redémarrage;

k) La version du logiciel.

(289) L'entrepreneur doit fournir au Canada un rapport mensuel présenté sous forme de tableau ou de graphique; ce rapport porte sur les activités du centre de services et indique ce qui suit :

a) Le nombre d'appels reçus;

b) Le nombre d'appels répondus;

c) Le nombre d'appels répondus après 20 secondes d'attente;

d) Le nombre d'appels abandonnés après 20 secondes d'attente;

e) Le nombre d'appels non répondus (abandonnés – signal d'occupation);

f) Le nombre d'appels abandonnés (l'utilisateur raccroche);

g) Le nombre de billets d'incident ouverts;

h) Le temps moyen de conversation lié aux appels répondus en secondes;

i) Le temps moyen en secondes avant de répondre à un appel;

j) Le temps moyen en secondes avant d'abandonner un appel;

k) Le temps moyen en file d'attente avant que les appels soient abandonnés;

l) Le temps d'attente maximal en file d'attente;

m) Le pourcentage d'appels répondus par rapport au nombre de billets d'incident ouverts;

n) Le pourcentage d'appels reçus par rapport au nombre de billets d'incident ouverts;

o) Le pourcentage d'appels non abandonnés par rapport au nombre d'appels reçus;

p) Le pourcentage d'appels abandonnés par rapport au nombre d'appels reçus.

(290) L'entrepreneur doit fournir au Canada un rapport sommaire mensuel portant sur l'ensemble des attaques, incidents ou événements anormaux détectés, suivis ou traités, et comprenant ce qui suit :

a) Les 25 vecteurs de menace les plus importants;

b) Les 25 services, protocoles ou applications ciblés les plus importants;

c) Les 10 provenances ou sources d'attaques les plus importantes;

d) Les 10 organisations clientes ciblées les plus importantes;

e) Les 25 types d'attaques ou d'incidents (p. ex. injection, hameçonnage, déni de service, attaques par script intersites, téléchargements « à la volée », etc.) les plus importants.

(291) L'entrepreneur doit fournir au Canada un rapport mensuel portant sur l'ensemble des attaques, incidents ou événements anormaux détectés, suivis ou traités, par organisation cliente, et comprenant ce qui suit :

a) Le numéro d'incident;

b) La date d'ouverture du billet d'incident;

c) La date de fermeture du billet d'incident;

d) L'état;

e) Le vecteur de menace;

f) Le service, le protocole ou l'application ciblée;

g) La provenance ou la source de l'attaque;

h) Le type d'attaque ou d'incident (p. ex. injection, hameçonnage, déni de service, attaques par script intersites, téléchargements « à la volée », etc.).

6.2 Rapports hebdomadaires

(292) L'entrepreneur doit fournir au Canada un rapport hebdomadaire qui recense toutes les activités de changement visant le SSGGC pour les deux semaines à venir, y compris une description des incidences sur le service (prise en charge des ouvertures de session, des enregistrements).

(293) L'entrepreneur doit fournir au Canada un rapport hebdomadaire qui décrit les résultats des demandes de changement exécutées la semaine précédente, les demandes prévues pour la prochaine semaine et les demandes de changement qu'il a soumises au Canada pour approbation.

6.3 Rapports quotidiens

(294) L'entrepreneur doit fournir au Canada un rapport quotidien présenté sous forme de tableau ou de graphique, et par organisation cliente; ce rapport indique ce qui suit :

a) Le nom de l'organisation cliente;

b) Le PPS;

c) La plateforme de service;

d) Les services de gestion des menaces offerts par la plateforme de service;

e) La date et l'heure du début;

f) La date et l'heure de la fin;

g) Le pourcentage de disponibilité depuis le début du mois;

h) Un résumé de la disponibilité depuis le début du mois, sous forme de graphique à colonnes, où :

i) Le jour du mois figure sur l'axe x;

ii) Le pourcentage de disponibilité figure sur l'axe y.

(295) L'entrepreneur doit fournir au Canada un rapport quotidien qui indique ce qui suit pour chaque capacité de gestion des menaces du SSGGC, sur le plan de la performance :

a) Le nom de l'organisation cliente;

b) Le PPS;

c) La plateforme de service;

d) Les services de gestion des menaces offerts par la plateforme de service;

e) La date et l'heure du début;

f) La date et l'heure de la fin;

g) L'utilisation moyenne et maximale de la mémoire;

h) L'utilisation moyenne et maximale du processeur;

i) L'utilisation moyenne et maximale de la bande passante;

j) La date du dernier redémarrage;

k) La version du logiciel.

6.4 Rapports spéciaux

(296) L'entrepreneur doit fournir au Canada un rapport spécial portant sur la détection d'atteintes à la sécurité; le rapport est ventilé selon la période de déclaration précisée par le Canada et porte sur ce qui suit :

a) Le nombre d'incidents de sécurité;

b) Le nombre d'enquêtes sur la sécurité complétées;

c) Le temps de réponse moyen et maximal aux incidents de sécurité;

d) Le temps d'exécution moyen et maximal des enquêtes sur la sécurité.

(297) L'entrepreneur doit fournir au Canada, dans les 72 heures suivant une demande, un rapport spécial rétrospectif portant sur l'incident de sécurité qui comprend ce qui suit, sans s'y limiter :

a) Le numéro d'incident;

b) La date d'ouverture du billet d'incident;

c) La date de fermeture du billet d'incident;

d) La description de l'incident;

e) La portée de l'incident;

f) La chaîne des événements ou l'échéancier;

g) Les mesures prises par le SSGGC;

h) Les leçons apprises;

i) Les limites ou problèmes liés au SSGGC;

j) Les recommandations visant l'amélioration du SSGGC.

(298) L'entrepreneur doit fournir au Canada un rapport spécial portant sur les atteintes à la vie privée; le rapport est ventilé selon la période de déclaration précisée par le Canada et porte sur ce qui suit :

a) Le nombre d'incidents liés à la protection de la vie privée;

b) Le nombre d'enquêtes réalisées sur la protection de la vie privée;

c) Le temps de réponse moyen et maximal lié aux incidents relatifs à la protection de la vie privée.

(299) L'entrepreneur doit fournir un rapport spécial portant sur tous les incidents de gravité élevée et faisant état des mesures de suivi des questions en suspens pertinentes.

(300) L'entrepreneur doit fournir au Canada, dans les cinq JOFPF suivant la modification de l'information contenue dans le rapport précédent, un rapport d'inventaire spécial décrivant l'équipement installé dans les sites du Canada pour le SSGGC. Le rapport doit indiquer :

a) L'équipement dont l'entrepreneur est propriétaire;

b) L'équipement dont le Canada est propriétaire;

c) L'équipement dont une tierce partie est propriétaire (cette tierce partie étant identifiée);

d) Le fabricant de l'équipement et son pays d'origine;

e) Le modèle et le numéro de série de l'équipement;

f) L'emplacement où chaque pièce d'équipement est installée en intégrant l'information aux diagrammes de réseau exigés dans la section portant sur la conception du service, de sorte que le Canada puisse, en passant en revue l'inventaire, immédiatement trouver dans le diagramme l'endroit où une pièce d'équipement a été déployée dans le réseau (et vice-versa);

g) La date d'installation de l'équipement;

h) La date du dernier entretien (préventif ou correctif) de l'équipement;

i) La date de la dernière mise à jour du micrologiciel.

(301) L'entrepreneur doit fournir au Canada, dans les 48 heures suivant la fermeture d'un billet d'incident, un rapport spécial comprenant ce qui suit :

a) Le numéro d'incident;

b) La date d'ouverture du billet d'incident;

c) La date de fermeture du billet d'incident;

d) La description de l'incident

e) Les facteurs déterminants (causes fondamentales) de l'incident;

f) Les recommandations visant l'amélioration du SSGGC.

(302) L'entrepreneur doit donner suite à une demande d'information que lui a présentée le Canada, selon la gravité que précise le Canada; la réponse que fournit l'entrepreneur comprend sans s'y limiter les renseignements suivants associés à un incident de sécurité, notamment :

a) Les résultats d'une recherche historique des journaux liés à une ou plusieurs organisations clientes, en fonction de critères fournis par le Canada dans un format de fichier commercial déterminé par le Canada;

b) Les résultats de l'analyse des journaux liés à une ou plusieurs organisations clientes, en fonction de critères fournis par le Canada dans un format de fichier commercial déterminé par le Canada;

c) Les journaux fondés sur des critères fournis par le Canada dans un format de fichier commercial déterminé par le Canada;

d) Les changements récents concernant la configuration;

e) Toute autre information ou donnée supplémentaire que précise le Canada.

(303) L'entrepreneur doit donner suite à une demande d'information que lui a présentée le Canada, selon la gravité de l'incident que précise le Canada; la réponse que fournit l'entrepreneur renferme une évaluation du niveau de protection que fournirait le SSGGC en fonction d'un scénario d'attaque ou de menace communiqué par le Canada (c'est-à-dire sommes-nous protégés contre ce type d'attaque ou de menace?).

7 SÉCURITÉ

(304) L'entrepreneur doit, dans le JOFPF qui suit une demande présentée par le Canada, lui fournir les registres de vérification en ligne relatifs au SSGGC dans les installations qu'il précise, dans un format de fichier commercial déterminé par le Canada.

(305) L'entrepreneur doit, dans les cinq JOFPF suivant une demande présentée par le Canada, lui fournir les registres de vérification archivés relatifs au SSGGC dans les installations qu'il précise, dans un format de fichier commercial déterminé par le Canada.

(306) L'entrepreneur doit conserver les registres portant sur les infractions à la sécurité, les transactions, les vérifications et les incidents d'alerte, ainsi que les rapports connexes, pour la période courante et les deux années précédentes, et il doit obtenir l'autorisation écrite du Canada pour les détruire après deux années.

(307) L'entrepreneur doit permettre au Canada ou à ses délégués de se rendre sans préavis dans ses locaux pour inspecter et vérifier sa conformité aux exigences prévues au contrat en matière de protection des renseignements personnels, de sécurité et de gestion de l'information, et d'avoir pleinement accès à tous dossiers et renseignements personnels de 8 h à 17 h HE les JOFPF, sans frais pour le Canada.

(308) En cas d'incident de sécurité, ou si le Canada en fait la demande autrement, l'entrepreneur doit prêter son concours à toute inspection ou vérification de la sécurité que demande le Canada en fournissant, selon la gravité que précise le Canada :

a) Toute documentation sur les flux de données, description des mécanismes de sécurité et de protection des données, et description de l'architecture des données se rapportant aux travaux prévus au présent contrat;

b) Ses propres évaluations des facteurs relatifs à la vie privée, énoncés de sensibilité, évaluations des menaces et des risques et plans de traitement des risques se rapportant aux travaux prévus au présent contrat;

c) L'accès aux documents, rapports, données et journaux concernant le SSGGC;

d) L'accès aux renseignements propres au SSGGC, disponibles par l'intermédiaire des postes de travail de direction de son réseau;

e) L'accès à ses employés et aux consultants indépendants pendant les heures de bureau (entre 8 h et 17 h HE) les JOFPF ou à d'autres moments convenus mutuellement, aux fins de réalisation d'entrevues par le Canada;

f) L'accès aux documents, pratiques et processus administratifs et opérationnels propres au SSGGC;

g) L’accès aux méthodes, sources de données et processus utilisés pour produire les rapports sur le SSGGC;

h) L’accès aux installations requises (port de réseau, console, etc.) afin que le Canada puisse effectuer une surveillance passive du SSGGC;

i) La MTES mise à jour.

(309) L’entrepreneur doit fournir l’accès à ses installations et systèmes, et transmettre, en temps opportun et en quantité suffisante, les documents et éléments de preuve, en lien avec le SSGGC, demandés par le Canada.

(310) L’entrepreneur doit, à l’intérieur du délai précisé par le Canada, prendre les mesures nécessaires pour atténuer les risques recensés dans l’application des processus de conformité du Canada en matière de sécurité et de protection des renseignements personnels et qui démontrent que les principes de sécurité et de protection des renseignements personnels du Canada ont été compromis, ou qu’ils sont susceptibles de l’être.

(311) L’entrepreneur doit mettre à jour les procédures d’exploitation de la sécurité, tel que le demande le Canada et à l’intérieur du délai qu’il précise, dans le cadre de ses activités continues d’amélioration des services.

(312) L’entrepreneur ne doit pas cacher au Canada toute information ou donnée qu’il détient et qui a trait au SSGGC ou à un incident de sécurité.

7.1 Examen de la conformité

(313) Le Canada réalisera, chaque année, un examen de la conformité visant à assurer ce qui suit, sans s'y limiter :

a) Le SSGGC se conforme aux exigences de sécurité pour le SSGGC (voir l'appendice A : Exigences de sécurité de l'annexe A au SSGGC);

b) Tous les logiciels du SSGGC comprennent les mises jour de sécurité et correctifs courants et à jour à l'égard des vulnérabilités connues;

c) L'entrepreneur surveille proactivement les vulnérabilités des logiciels du SSGGC et met en œuvre les correctifs de sécurité ou versions de logiciel requis pour remédier à de telles vulnérabilités;

d) L'entrepreneur examine quotidiennement les enregistrements figurant dans les registres de vérification de la sécurité.

(314) L'entrepreneur doit, dans les 10 JOFPF suivant une demande présentée par le Canada, fournir toute preuve exigée à l'appui de l'examen de la conformité.

(315) S'il estime que ces preuves n'appuient pas la conformité de l'entrepreneur aux modalités du contrat, le Canada lui demandera de soumettre un plan visant à remédier aux écarts observés.

8 NIVEAUX DE SERVICE

(316) L'entrepreneur doit respecter ou dépasser les niveaux de service.

(317) L'entrepreneur doit surveiller, mesurer et calculer les niveaux de service en tout temps (24 heures sur 24, sept jours sur sept, 365 jours par année).

(318) L'entrepreneur doit fournir le matériel et (ou) les logiciels nécessaires pour surveiller et mesurer les niveaux de service.

(319) L'entrepreneur ne doit pas inclure les mesures relatives aux niveaux de service manqués dans le calcul des niveaux de service.

(320) L'entrepreneur doit comptabiliser les mesures de performance liées aux niveaux de service omis comme étant des mesures ratées.

(321) L'entrepreneur doit calculer et signaler les niveaux de service arrondis à deux décimales près, à moins d'indication contraire.

8.1 Niveau de service lié à la disponibilité du portail de services

(322) Le niveau de service lié à la disponibilité du portail de services (NS-DPS) doit être inférieur ou égal à une heure (soit l'équivalent approximatif d'une disponibilité de 99,85 %) du temps d'interruption cumulé pendant toute période de 24 heures, soit tous les jours, au cours de tout mois civil donné.

(323) Le NS-DPS correspond au total du temps d'interruption au cours du mois civil.

(324) Le temps d'interruption relatif au portail de services comprend l'un ou l'autre des éléments suivants :

a) Les périodes pendant lesquelles le portail de services n'est pas opérationnel, de sorte que le Canada ne peut pas accéder aux données, rapports ou fonctions administratives qu'il contient;

b) Les temps de réponse en ligne liés au portail de services qui dépassent les temps de réponse maximaux approuvés par le Canada.

(325) Le temps d'interruption relatif au portail de services ne tient pas compte des périodes de maintenance planifiées approuvées par le Canada ni du temps associé aux changements d'urgence qu'il faut faire pour rétablir le portail, sur le plan opérationnel, par suite d'un état défavorable, d'une dégradation du service ou d'une défaillance.

(326) L'entrepreneur doit exécuter tous les travaux de maintenance prévus pour le portail de services pendant les périodes de maintenance approuvées par le Canada.

(327) Le Canada ne refusera pas déraisonnablement d'approuver les périodes de maintenance que demande l'employeur à l'égard du portail de services.

8.2 Niveau de service lié au temps de réponse du centre de services

(328) Le niveau de service lié au temps de réponse du centre de services (NS-TRCS) exige que 80,00 % de l'ensemble des appels téléphoniques reçus au cours d'un mois civil soient répondus dans les 20 secondes.

(329) Le NS-TRCS doit être calculé comme suit :

(nombre d'appels répondus dans les 20 secondes + nombre d'appels abandonnés dans les 20 secondes) / (nombre total d'appels répondus + nombre total d'appels abandonnés) * 100

(330) Le calcul du temps nécessaire pour répondre à un appel commence au moment où l'appel téléphonique est relayé au système téléphonique de l'entrepreneur et se termine au moment où un agent de son centre de services y répond.

(331) Un appel abandonné s'entend d'un appel téléphonique qui a été relayé au système téléphonique de l'entrepreneur et auquel l'appelant met fin avant qu'un agent du centre de services y réponde.

8.3 Niveau de service lié à la mise en attente par le centre de services

(332) Le niveau de service lié à la mise en attente par le centre de services (NS-MACS) ne doit pas dépasser 30 secondes pour 90,00 % de l'ensemble des appels téléphoniques que reçoit le centre de services au cours d'un mois civil.

(333) L'entrepreneur doit calculer le NS-MACS depuis le moment où un agent du centre de services met en attente un appel jusqu'au moment où il retire cet appel de la mise en attente.

(334) Le NS-MACS doit être calculé comme suit :

(appels mis en attente respectant le niveau de service + appels sans mise en attente) / nombre total d'appels * 100

8.4 Niveau de service lié au temps de réponse

(335) Le niveau de service lié au temps de réponse (NS-TR) s'appliquant à une capacité de gestion des menaces du SSGGC à un PPS ne doit pas être inférieur à 95,00 % de la

vitesse filaire relative à cette capacité pendant plus de trois minutes (soit l'équivalent approximatif de 95,00 % du temps selon une vitesse filaire de 95,00 % et plus) au cours de chaque heure (p. ex. de 7 h à 8 h [HE]) de chaque JOFPF pris en compte dans la période de crédit de service du NS-TR (soit de 7 h à 19 h [HE]) pour chaque jour au cours d'un mois civil.

8.5 Niveau de service lié au temps d'interruption maximal du service

(336) Le premier niveau de service lié au temps d'interruption maximal du service (NS-TIMS1) doit être inférieur ou égal à 3,6 heures (soit l'équivalent approximatif d'une disponibilité de 99,50 %) du temps d'interruption cumulé pendant toute période de 24 heures, soit tous les jours, au cours de tout mois civil donné à un PPS.

(337) Le deuxième niveau de service lié au temps d'interruption maximal du service (NS-TIMS2) doit être inférieur ou égal à 43,2 minutes (soit l'équivalent approximatif d'une disponibilité de 99,90 %) du temps d'interruption cumulé pendant toute période de 24 heures, soit tous les jours, au cours de tout mois civil donné à un PPS.

(338) L'entrepreneur doit calculer les NS-TIMS1 et NS-TIMS2 à l'égard du SSGGC en additionnant le temps d'interruption relatif à tous les incidents qui suivent, observé à un PPS, pour le mois civil en question :

a) La capacité du SSGGC en matière du GIES n'est pas fonctionnelle;

b) La capacité de gestion des menaces du SSGGC n'est pas fonctionnelle;

c) N'importe quel service de gestion des menaces du SSGGC n'est pas fonctionnel;

d) Le SSGGC ne filtre pas correctement le trafic entrant;

e) Le SSGGC ne filtre pas correctement le trafic sortant;

f) Le NS-TR est raté plus de cinq fois consécutives;

g) Le NS-TR est raté plus de trois fois au cours d'une heure donnée (le temps d'interruption est calculé à partir du moment où le premier NS-TR est raté dans l'heure donnée jusqu'au moment où le dernier NS-RT est raté dans la même heure).

(339) Le calcul du NS-TIMS1 et celui du NS-TIMS2 ne doivent pas tenir compte du temps d'interruption lié aux événements qui suivent :

a) La défaillance des équipements ou des installations situées à un PPS et dont l'entrepreneur est propriétaire et gestionnaire, lorsque cette défaillance résulte de dommages causés par une partie autre que l'entrepreneur ou est attribuable au retrait, au déménagement ou à l'altération des équipements ou installations par une telle partie;

b) La défaillance d'un service qui n'est pas fourni par l'entrepreneur;

c) Les problèmes de configuration des postes de travail autorisés par le Canada;

d) Les périodes de maintenance approuvées par le Canada.

8.6 Niveau de service lié au délai maximal de rétablissement du service

(340) Le premier niveau de service lié au délai maximal de rétablissement du service (NS-DMRS1) est de 15 minutes.

(341) Le deuxième niveau de service lié au délai maximal de rétablissement du service (NS-DMRS2) est de 30 minutes.

(342) Le calcul du NS-DMRS1 ou du NS-DMRS2 commence à compter du moment où le Canada ou l'entrepreneur détectent un incident, pour lequel le NS-TIMS est calculé, touchant le SSGGC à un PPS, jusqu'au moment où le billet d'incident est fermé.

(343) Le calcul du NS-DMRS se poursuit pour chaque incident comportant une période d'interruption peu importe si le NS-TIMS a été dépassé ou non au cours d'un mois civil.

8.7 Niveau de service lié au temps de réponse à une autorisation de tâches

(344) Le niveau de service lié au temps de réponse à une autorisation de tâches (NS-TRAT) doit être inférieur ou égal aux délais de prestation de service, déterminés par catégorie d'autorisation de tâches et précisés dans le tableau 1.

Tableau 1 Réponse à une autorisation de tâches

CATÉGORIE D'AUTORISATION DE TÂCHES	DÉLAI DE PRESTATION DE SERVICE SELON LA TAILLE DE L'INSTALLATION EN JOFPF			
	PETITE	MOYENNE	GRANDE	TRÈS GRANDE
Installer une capacité de gestion des menaces du SSGGC, à un PPS, ainsi que les services initiaux de gestion des menaces du SSGGC	20	20	20	40
Ajouter un service de gestion des menaces du SSGGC	5	5	10	20

(345) L'entrepreneur doit calculer le NS-TRAT comme étant le nombre de JOFPF s'écoulant entre la date à laquelle le Canada délivre l'autorisation de tâches à l'entrepreneur et l'acceptation du travail par le Canada. Pour obtenir les détails relatifs à la taille de l'installation (petite, moyenne, grande, très grande) indiquée dans le tableau 1 ci-dessus, voir les profils des fonctions figurant dans les tableaux C et D de l'annexe B : Base de paiement au document de demande de soumissions.

8.8 Niveau de service lié au temps de réponse à une demande de changement

(346) Le niveau de service lié au temps de réponse à une demande de changement (NS-TRDC) doit être inférieur ou égal aux délais relatifs au temps de réponse à une demande de changement, déterminés par catégorie de demande de changement et précisés dans le tableau 2.

Tableau 2 Réponse à une demande de changement

CATÉGORIE DE DEMANDE DE CHANGEMENT	TRDC STANDARD (heures par JOFPF)	TRDC D'URGENCE (24 heures sur 24, sept jours sur sept, 365 jours par année)
Création de nouvelles politiques, règles, listes blanches et listes noires configurées, ou mise à jour de celles-ci	24 heures	4 heures
Création de nouvelles signatures de menace configurées ou mise jour de celles-ci	24 heures	4 heures
Autre changement	Prochaine période de maintenance planifiée	4 heures

(347) L'entrepreneur doit calculer le NS-TRDC à l'égard d'une demande de changement comme étant la période de temps écoulée entre l'émission de la demande de changement par le Canada et la fermeture du billet de changement correspondant.

9 NORMES

9.1 Ethernet rapide

(348) Les normes et fonctionnalités qui suivent s'appliquent à l'Ethernet rapide :

a) L'Ethernet rapide conformément à la norme IEEE 802.3 à 10/100 Mbps;

b) IEEE 802.1Q;

c) IEEE 802.3ac;

d) IEEE 802.3ad;

e) Le câblage selon ce que précise le Canada : câblage 100Base-TX ou câblage 100Base-SX;

f) Les connecteurs selon ce que précise le Canada : 8P8C, communément appelé RJ-45; ou connecteur SC conformément à la norme FOCIS 3 dans EIA/TIA 604-03; ou connecteur MT-RJ, conformément à la norme FOCIS 12 dans EIA/TIA-604-12.

9.2 Gigabit Ethernet

(349) Les normes et fonctionnalités qui suivent s'appliquent au Gigabit Ethernet :

a) Gigabit Ethernet conformément aux normes IEEE 802.3ab et IEEE 802.3z à 1 000 Mbps;

b) Le taggage de RLV conformément à la norme IEEE 802.3ac;

c) IEEE 802.1Q;

d) IEEE 802.3ac;

e) IEEE 802.3ad;

f) Le câblage selon ce que précise le Canada : câblage 1000Base-T ou câblage 1000Base-SX;

g) Les connecteurs selon ce que précise le Canada : connecteurs modulaires 8P8C, communément appelés RJ-45; ou connecteur SC conformément à la norme FOCIS 3 dans EIA/TIA-604-03; ou connecteur MT-RJ, conformément à la norme FOCIS 12 dans EIA/TIA-604-12.

9.3 Protocole Internet

(350) Les normes et fonctionnalités qui suivent s'appliquent au protocole Internet :

a) IPv4 [RFC 791];

b) IPv6 [RFC 2460] y compris :

i) L'encapsulation de IPv6 sur les réseaux IPv4;

ii) Les réseaux IPv6 natifs.

(351) IPv4 et IPv6 doivent être pris en charge concurremment.

9.4 Protocole TLS

(352) Les normes et fonctionnalités qui suivent s'appliquent au protocole TLS :

a) La plus récente version du protocole TLS (version 1.0 [RFC 2246] ou version 1.1 [RFC 4346] ou version 1.2 [RFC 5246]) offerte sur le marché par le fabricant du matériel et du logiciel fournis par l'entrepreneur pour le SSGGC;

b) Les versions subséquentes du protocole TLS dans les trois mois suivant une demande présentée par le Canada, lorsque celles-ci sont offertes sur le marché par le fabricant du matériel et du logiciel fournis par l'entrepreneur pour le SSGGC, sans coûts additionnels pour le Canada;

c) L'extension d'indication de renégociation TLS [RFC 5746];

d) L'interdiction de la version 2.0 du protocole SSL [RFC 6176].

9.5 Protocole de sécurité IP

(353) Les normes et fonctionnalités qui suivent s'appliquent au protocole de sécurité IP (IPsec) :

a) L'architecture de sécurité pour le protocole Internet [RFC 4301];

b) Le code d'authentification de message haché par clé (HMAC) [FIPS 198-1];

c) L'encapsulation IP ESP (IP Encapsulating Security Payload) [RFC 4303];

d) La version 2 de l'échange de clés Internet (IKEv2) [RFC 4306].

10 INTÉGRATION ET SOUTIEN TECHNIQUE

(354) L'entrepreneur doit fournir au Canada, à la demande de celui-ci, une personne-ressource pour le soutien technique à l'intégration, comme il est demandé dans une autorisation de tâches délivrée par le Canada, pour effectuer sur demande les tâches suivantes :

a) Fournir de l'information sur les aspects techniques du SSGGC et des directives sur les spécifications techniques qui s'appliquent à l'intégration et à l'évolution de la technologie de gestion des menaces;

b) Fournir un soutien technique et des conseils relativement à la configuration et à l'évolution des mécanismes de gestion des menaces;

c) Fournir un soutien technique en cas de problèmes liés à la technologie de gestion des menaces;

d) Élaborer de la documentation sur l'intégration et l'évolution des mécanismes de gestion des menaces;

e) Fournir des directives relativement aux problèmes de sécurité associés aux mécanismes de gestion des menaces.

(355) La personne-ressource pour le soutien à l'intégration doit posséder les qualifications minimales suivantes :

a) 2 années d'expérience en gestion des menaces, volet technologie;

b) 2 années d'expérience en gestion des menaces, volet sécurité;

c) 2 années d'expérience dans la prestation d'un soutien et de conseils techniques relativement à l'intégration et à l'évolution de la technologie de gestion des menaces au sein d'équipes multidisciplinaires opérationnelles, techniques et de projet.

(356) L'entrepreneur doit fournir au Canada, à la demande de celui-ci, un gestionnaire de l'intégration chargé du soutien à l'intégration, comme il est demandé dans une autorisation de tâches délivrée par le Canada, pour effectuer les tâches suivantes :

a) Créer, mettre à jour et gérer les plans de projet d'intégration et d'évolution, y compris les jalons, les produits livrables et les risques;

b) Fournir des conseils quant aux meilleures pratiques à adopter à l'égard des initiatives d'intégration et d'évolution;

c) Déterminer les risques liés à l'intégration et à l'évolution et préparer des plans d'atténuation;

d) Déterminer et consigner les exigences et les observations en matière d'intégration et d'évolution;

e) Coordonner les équipes de soutien (préparation visant le réseau, la sécurité, les opérations, les ordinateurs de bureau, la gestion des menaces) en vue des initiatives d'intégration et d'évolution;

f) Suivre l'avancement des initiatives d'intégration et d'évolution.

(357) Le gestionnaire de l'intégration doit posséder les qualifications minimales suivantes :

a) Certification PMP;

b) Certification ITIL (de base);

c) 2 années d'expérience en sécurité des TI;

d) 2 années d'expérience en gestion des services de TI;

e) 2 années d'expérience en gestion d'équipes multidisciplinaires opérationnelles, techniques et de projet.

11 FORMATION

(358) L'entrepreneur doit fournir une formation Web (FW) de sensibilisation à la sécurité.

(359) L'entrepreneur doit offrir la FW au moyen d'un système de gestion de l'apprentissage (SGA) sécurisé.

(360) L'entrepreneur doit héberger le SGA.

(361) L'entrepreneur doit fournir au Canada un SGA comprenant ce qui suit :

a) La marque du Canada;

b) La conformité aux Règles pour l'accessibilité des contenus Web 2.0 (WCAG 2.0) du consortium W3C, niveau AA, règles 1 et 2 (http://www.w3.org/Translations/WCAG20-fr/);

c) L'accès au moyen d'un navigateur Web pour au moins 5 000 sessions simultanées;

d) L'accès sécurisé des utilisateurs grâce à :

i) Une connexion d'accès sécurisée (par exemple le protocole TLS);

ii) L'accès HTTPS à l'aide des certificats approuvés par le navigateur Web;

iii) Un nom d'utilisateur et un mot de passe uniques;

iv) L'obligation de modifier le mot de passe après le premier accès, et à des intervalles réguliers par la suite, conformément aux politiques de sécurité du SSGGC;

v) La désactivation des comptes d'utilisateur après de multiples tentatives infructueuses de fournir le bon mot de passe, d'après une politique précisée par le Canada;

vi) La désactivation de comptes d'utilisateur pour cause d'inactivité, d'après une politique précisée par le Canada;

vii) La présentation d'une question d'identification en cas d'oubli de mot de passe. Une bonne réponse à la question doit se solder par l'envoi par courriel d'un nouveau mot de passe à l'utilisateur;

viii) L'accès réservé aux utilisateurs autorisés et approuvés par le Canada;

ix) L'accès réservé aux utilisateurs authentifiés à l'aide d'un justificatif approuvé par le Canada;

x) La récupération des justificatifs en libre-service, à l'aide d'une méthode approuvée par le Canada;

e) Une page d'orientation ou d'introduction;

f) L'aide en ligne et les coordonnées pertinentes;

g) Un glossaire complet;

h) L'accès par Internet;

i) Un fonctionnement adéquat en utilisant une combinaison des systèmes d'exploitation et des navigateurs les plus populaires;

j) Une interface conviviale dotée d'options et de menus intuitifs présentés en langage clair et simple et structurés de façon logique;

k) L'entrée de données assistée où des zones d'entrée contenant des valeurs prédéfinies sont remplies au moyen de listes, déroulantes ou non, de cases à cocher et de boutons radio présentés en langage clair et simple;

l) La vérification des erreurs lorsque les zones d'entrée sont examinées pour en confirmer le format ou la validité, y compris la validation croisée des zones; les messages d'erreur sont détaillés, rédigés en langage clair et simple et indiquent à l'utilisateur ce qui est incorrect et les règles qui n'ont pas été satisfaites;

m) L'affichage du texte ou des pages d'aide ou du texte ou des commandes de navigation, dans la langue préférée (français ou anglais) de l'utilisateur précisée dans le profil utilisateur;

n) La modification par l'utilisateur de la langue de l'interface utilisateur.

(362) Le matériel de la FW doit être disponible en français et en anglais.

(363) Le matériel de la FW doit être approuvé par le Canada.

(364) Le matériel de la FW doit être conforme aux politiques suivantes du Secrétariat du Conseil du Trésor du Canada :

a) *Politique sur la sécurité du gouvernement*;

b) *Directive sur la gestion de la sécurité ministérielle*;

c) Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information;

d) *Norme opérationnelle sur la sécurité matérielle*;

e) *Norme sur la sécurité du personnel*;

f) *Politique sur la protection de la vie privée*.

(365) Le matériel de la FW doit être disponible pour les groupes suivants visés par la formation :

a) Les utilisateurs finals;

b) Les gestionnaires;

c) Les administrateurs de TI.

(366) Le matériel de la FW destiné aux utilisateurs finals doit traiter des sujets suivants :

a) Les éléments de base de la sécurité de l'information, selon la *Politique sur la sécurité du gouvernement*;

b) La gestion des menaces et des risques;

c) La classification de l'information;

d) La gestion de l'information;

e) La propriété intellectuelle;

f) Les mots de passe;

g) La sécurité matérielle et la sécurité des supports mobiles;

h) Le courrier électronique;

i) Les messages électroniques non sollicités (pourriels);

j) La confidentialité sur le Web;

k) Les communications externes;

l) La mise en sécurité des documents;

m) La protection des renseignements personnels;

n) La protection des cartes de paiement;

o) Les logiciels malveillants (virus, vers, chevaux de Troie et logiciels espions);

p) Le piratage psychologique;

q) Les réseaux sociaux;

r) Le vol d'identité;

s) Les utilisateurs mobiles;

t) La destruction de l'information sensible;

u) Le télétravail.

(367) Le matériel de la FW destiné aux gestionnaires doit traiter des sujets suivants :

a) La formation des utilisateurs finals sous l'angle du rôle du gestionnaire et du Cadre de responsabilité de gestion;

b) Les politiques concernant la gouvernance et la sécurité;

c) Les principaux rôles qu'assument les gestionnaires dans le cadre des programmes de sensibilisation à la sécurité;

d) La détermination des rôles et responsabilités des gestionnaires pour assurer l'application des meilleures pratiques organisationnelles;

e) La réponse aux incidents;

f) Les plans de reprise après sinistre.

(368) Le matériel de la FW destiné aux administrateurs de TI doit traiter des sujets suivants :

a) La formation des utilisateurs finals sous l'angle de la sécurité des TI, en ce qui a trait aux réseaux et aux bases de données;

b) Les vulnérabilités et les menaces;

c) Les attaques types contre les réseaux;

d) Les attaques conventionnelles;

e) Les divers types d'attaques;

f) Les pare-feu;

g) Les zones démilitarisées et autres zones de service;

h) Les réseaux privés virtuels;

i) Le protocole IPsec;

j) Les protocoles SSL ou IPSec;

k) La prévention et la détection des intrusions;

l) Les principales menaces;

m) La cryptographie;

n) Le chiffrement et la sécurité;

o) Le code d'authentification de message;

p) La fonction de hachage;

q) Le chiffrement à clé publique;

r) Les signatures numériques.

(369) Le matériel que fournit l'entrepreneur à l'égard de la FW est adapté à la sensibilisation à la sécurité pour les groupes visés par la formation, tel que le précise le Canada dans l'autorisation de tâches; au besoin, l'entrepreneur traite de sujets nouveaux ou actualisés approuvés par le Canada.

(370) Les sujets traités dans le matériel de la FW doivent être répartis en modules autonomes.

(371) Le matériel de la FW doit prévoir des évaluations d'apprentissage, chaque module comportant un choix de questions d'évaluation.

(372) Le SGA doit permettre à un administrateur de personnaliser les cours de la FW en choisissant une combinaison de modules et de sujets existants et en leur attribuant un ordre de livraison.

(373) Le SGA doit permettre à un administrateur de personnaliser les évaluations des cours de la FW en choisissant des questions d'évaluation liées aux sujets traités dans le cours.

(374) Le SGA doit permettre d'effectuer l'évaluation à la fin du cours et de noter les résultats sans consigner de renseignements sur l'utilisateur.

(375) Le SGA doit permettre à un administrateur de réaliser un sondage en :

a) Concevant un questionnaire à partir d'une liste de questions prédéfinies et de questions personnalisées;

b) Définissant la méthode de réponse prévue : oui ou non; vrai ou faux; choix multiples, etc.;

c) Déterminant la bonne réponse.

(376) Le SGA doit permettre à l'utilisateur de répondre au sondage, de noter les résultats chaque fois que le sondage est réalisé, et ce, sans consigner de renseignements concernant son identité.

(377) Le SGA doit informer l'utilisateur que le résultat qu'il a obtenu demeurera confidentiel.

(378) L'entrepreneur doit fournir au Canada, à la suite de la mise en œuvre du SGA, un exemplaire électronique du guide de l'utilisateur concernant le SGA, qui documente ce qui suit :

a) Les instructions relatives à la structure, au contenu et à l'utilisation du SGA;

b) Les copies d'écran relatives aux menus, entrées de données et rapports.

(379) L'entrepreneur doit sauvegarder toute l'information concernant le SGA quotidiennement et conserver les sauvegardes quotidiennes dans un emplacement hors site pendant trois ans.

(380) Le SGA doit permettre d'accéder à l'ensemble de l'information la concernant des trois années précédentes.

(381) Le SGA doit permettre à un utilisateur authentifié d'accéder à toutes les pages et fonctions du SGA auxquelles il est autorisé, sans qu'il ait à s'authentifier davantage après son authentification initiale, et ce, jusqu'à ce qu'il ferme la session ou que celle-ci expire.

(382) Le SGA doit enregistrer tous les accès au système et fournir au Canada un fichier électronique des enregistrements des journaux d'accès pour les 12 mois précédents, en respectant la convention régissant les noms de fichier dictée par le Canada et le format de fichier commercial approuvé par le Canada.

(383) Le SGA doit permettre l'autoenregistrement et l'inscription en ligne des utilisateurs, sur invitation; cette démarche prévoit ce qui suit :

a) La diffusion par courriel d'invitations à s'enregistrer sur une liste d'adresse de courriel fournie par le Canada, en appliquant une méthode approuvée par celui-ci;

b) L'inscription automatique dans un groupe par défaut visé par la formation, selon ce que précise le Canada au moment de l'enregistrement;

c) La diffusion par courriel d'invitations à s'inscrire à une liste d'adresses de courriel, fournie par le Canada, visant d'autres types de groupes visés par la formation (gestionnaires; administrateurs de TI), selon une méthode approuvée par celui-ci;

d) La prévention de tentatives d'enregistrement non autorisées, selon une méthode approuvée par le Canada;

e) La prévention de tentatives d'inscription non autorisées, selon une méthode approuvée par le Canada;

f) L'autoenregistrement des utilisateurs ayant reçu une invitation à s'enregistrer;

g) Un système automatisé de distribution par courriel qui envoie les courriels visant l'enregistrement uniquement aux domaines de courriel autorisés de l'organisation cliente;

h) Un système automatisé de distribution par courriel qui envoie les courriels visant l'inscription uniquement aux utilisateurs enregistrés de l'organisation cliente.

(384) Les profils utilisateurs du SGA doivent comprendre ce qui suit :

a) L'ID utilisateur et le mot de passe;

b) L'adresse de courriel;

c) La préférence linguistique (français ou anglais);

d) La liste des groupes inscrits et visés par la formation (utilisateurs finals, gestionnaires, administrateurs de TI);

e) Le nom de l'organisation cliente;

f) L'information portant sur la récupération des justificatifs, notamment les questions et réponses d'identification.

(385) Le SGA doit permettre l'accès distinct aux cours par groupe visé par la formation.

(386) Le SGA doit permettre l'accès distinct aux cours par programme d'apprentissage.

(387) L'entrepreneur doit créer des comptes d'administrateurs visant le SGA, dans les deux JOFPF suivant une demande présentée par le Canada à cet effet.

(388) Le SGA doit permettre à un utilisateur possédant le privilège d'administrateur de :

a) Créer, modifier et supprimer :

i) Les comptes d'administrateur;

ii) Les comptes d'utilisateur;

iii) Les groupes visés par la formation;

iv) Les programmes d'apprentissage;

v) Les renseignements concernant les organisations clientes.

b) Attribuer des comptes d'utilisateur aux organisations clientes;

c) Réactiver ou désactiver les comptes d'utilisateur;

d) Interroger et visualiser les profils utilisateur;

e) Assigner les cours de la FW aux groupes visés par la formation;

f) Assigner les cours de la FW aux programmes d'apprentissage;

g) Produire diverses statistiques concernant la FW.

(389) La SGA doit ventiler les données de façon logique par organisation cliente.

(390) Le SGA doit permettre l'administration déléguée dans les cas où un utilisateur possédant les privilèges d'administrateur ne pourrait accéder qu'à l'information (profils utilisateur, rapports, données et documents) que contient le système au sujet de l'organisation qui lui a été assignée.