Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
T8080-200405
Security Classification / Classification de sécurité Unclassified

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Transport Canada	2. Branch or Directorate / Direction générale ou Direction: Innovation Center
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Increase cyber readiness of transportation infrastructure owners and operators (IOO). Plan to achieve that by raising the cybersecurity awareness through development of briefing materials and cybersecurity primer, develop tools and guidance, consult stakeholders and deliver technical support and training sessions for IOO. First contract options provide additional as-needed basis stakeholder consultation, training sessions and technical support session. Second contract option provides strategic advice and cybersecurity analysis on emerging technologies. Third option is to perform penetration testing on selected transportation equipment.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis: No access to Transport Canada facilities or systems.		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada		**NATO / OTAN**		**Foreign / Étranger**	
	✓				

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion: ☑	All NATO countries / Tous les pays de l'OTAN: ☐	No release restrictions / Aucune restriction relative à la diffusion: ☐
Not releasable / À ne pas diffuser: ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A: ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ: ☐	PROTECTED A / PROTÉGÉ A: ☐
PROTECTED B / PROTÉGÉ B: ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE: ☐	PROTECTED B / PROTÉGÉ B: ☐
PROTECTED C / PROTÉGÉ C: ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL: ☐	PROTECTED C / PROTÉGÉ C: ☐
CONFIDENTIAL / CONFIDENTIEL: ☐	NATO SECRET / NATO SECRET: ☐	CONFIDENTIAL / CONFIDENTIEL: ☐
SECRET / SECRET: ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET: ☐	SECRET / SECRET: ☐
TOP SECRET / TRÈS SECRET: ☐		TOP SECRET / TRÈS SECRET: ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT): ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT): ☐

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No ☐ / Yes ☑
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ / Oui ☑
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No ☐ / Yes ☑
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? — Non ☐ / Oui ☑

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS COTE DE FIABILITÉ	☐ CONFIDENTIAL CONFIDENTIEL	☑ SECRET SECRET	☐ TOP SECRET TRÈS SECRET
☐ TOP SECRET– SIGINT TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL NATO CONFIDENTIEL	☐ NATO SECRET NATO SECRET	☐ COSMIC TOP SECRET COSMIC TRÈS SECRET
☐ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : For specific work elements and contract options, different security requirements may apply.

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No ☐ / Yes ☑
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? — Non ☐ / Oui ☑
If Yes, will unscreened personnel be escorted? — No ☐ / Yes ☑
Dans l'affirmative, le personnel en question sera-t-il escorté? — Non ☐ / Oui ☑

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No ☐ / Yes ☑
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ / Oui ☑

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No ☐ / Yes ☑
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? — Non ☐ / Oui ☑

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No ☐ / Yes ☑
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? — Non ☐ / Oui ☑

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No ☐ / Yes ☑
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ / Oui ☑

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No ☐ / Yes ☑
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale? — Non ☐ / Oui ☑

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ A	 B	 C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRES SECRET
Information / Assets Renseignements / Biens	✓	✓														
Production																
IT Media / Support TI	✓	✓														
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
T8080-200405
Security Classification / Classification de sécurité Unclassified

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Haydar Issa	Engineer, Environmental Programs	

Telephone No. - Nº de téléphone	Facsimile No. - Nº de télécopieur	E-mail address - Adresse courriel	Date
(343) 542-3175		haydar.issa@tc.gc.ca	October 27, 2020

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Gerry Babcock	Manager, Cyber Security, Digital Services Directorate	Babcock, Gerry L. Digitally signed by Babcock, Gerry L. Date: 2020.11.17 15:33:13 -05'00'

Telephone No. - Nº de téléphone	Facsimile No. - Nº de télécopieur	E-mail address - Adresse courriel	Date
613-990-5531		Gerry.Babcock@tc.gc.ca	2020-11-17

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?
☐ No / Non ☑ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Kristen Scott	Contracting Specialist	Scott, Kristen Digitally signed by Scott, Kristen DN: C=CA, O=GC, OU=TC-TC, OU=ATR-RAT, CN="Scott, Kristen" Reason: I am approving this document Location: your signing location here Date: 2020-12-14 12:24:39 Foxit PhantomPDF Version: 10.0.1

Telephone No. - Nº de téléphone	Facsimile No. - Nº de télécopieur	E-mail address - Adresse courriel	Date
506-377-2564		kristen.scott@tc.gc.ca	

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - Nº de téléphone	Facsimile No. - Nº de télécopieur	E-mail address - Adresse courriel	Date

Guide de classification de la sécurité de la GI/TI pour définir les niveaux d'habilitation de sécurité pour T8080-200405 – AMÉLIORER L'ÉTAT DE PRÉPARATION EN MATIÈRE DE CYBERSÉCURITÉ DU RÉSEAU DE TRANSPORT ROUTIER DU CANADA POUR DES NIVEAUX DE CONNECTIVITÉ ET D'AUTOMATISATION PLUS ÉLEVÉS

Les niveaux d'habilitation de sécurité suivants sont requis pour le contrat d'accompagnement selon la description du travail à effectuer dans l'énoncé de travail/le mandat fourni à la sécurité de la GI/TI. La liste de vérification des exigences de sécurité choisie pour ce contrat offre plus d'un niveau d'habilitation de sécurité.

Numéro du contrat :	T8080-200405
Titre du contrat :	AMÉLIORER L'ÉTAT DE PRÉPARATION EN MATIÈRE DE CYBERSÉCURITÉ DU RÉSEAU DE TRANSPORT ROUTIER DU CANADA POUR DES NIVEAUX DE CONNECTIVITÉ ET D'AUTOMATISATION PLUS ÉLEVÉS

Niveaux d'habilitation de sécurité requis :

Justification des niveaux requis si plus d'un niveau est requis :

Niveau	Nombre requis	Justification
☑ Reliability Fiabilité	3	Au besoin. EXEMPLES – *Une habilitation de niveau Fiabilité sera requise lorsqu'on accédera à des niveaux protégés d'information sur le site. Notez que l'entrepreneur n'aura accès à aucun actif du niveau protégé C ou Confidentiel.*
☐ Confidential Confidentiel		

Guide de classification de la sécurité de la GI/TI pour définir les niveaux d'habilitation de sécurité pour T8080-200405 – AMÉLIORER L'ÉTAT DE PRÉPARATION EN MATIÈRE DE CYBERSÉCURITÉ DU RÉSEAU DE TRANSPORT ROUTIER DU CANADA POUR DES NIVEAUX DE CONNECTIVITÉ ET D'AUTOMATISATION PLUS ÉLEVÉS

☑ Secret	3	Au besoin. EXEMPLES – *Une habilitation de niveau Secret sera requise lorsqu'on accédera à des niveaux Protégé ou Classifié d'information sur le site. Notez que l'entrepreneur n'aura accès à aucun actif du niveau protégé C ou Confidentiel.*
☐ Top Secret		

Guide de sécurité pour entrepreneurs qui utilisent les installations et le matériel informatique pour la production, le stockage et le traitement de renseignements électroniques protégés cotés B et pour l'accès à ces renseignements

Les entrepreneurs de Transport Canada (TC) qui utilisent leurs installations et leur matériel informatique pour traiter, stocker des renseignements confidentiels protégés cotés B, et pour y avoir accès, sont tenus d'observer les critères ci-après et des renseignements détaillés sur la configuration STIde leurs systèmes et de leurs installations aux services de GI-TI de Transport Canada.

Exigences:

1. Les entrepreneurs doivent autoriser Transport Canada (TC) à effectuer l'inspection et la vérification de l'infrastructure en technologie de l'information si nécessaire.

2. Employés des partenaires ou des tierces parties:
   2.1. Les employés (y compris les entrepreneurs) qui ont accès à des renseignements protégés cotés B ou qui fournissent des services administratifs, de soutien ou de maintenance pour l'infrastructure en technologie de l'information ou ses produits d'information doivent posséder une cote d'autorisation de vérification de fiabilité approfondie minimale, en conformité avec la Norme sur la sécurité du personnel du Secrétariat du Conseil du Trésor.

3. Les entrepreneurs doivent observer les mesures de contrôle administratives, les concepts et la philosophie de gestion du risque énoncés dans la Norme opérationnelle de sécurité –Gestion de la sécurité des technologies de l'information (GSTI):
   3.1. modification des processus de contrôle et de gestion visant l'approbation des changements apportés au matériel et aux logiciels;
   3.2. gestion de la configuration –définie et documentée;
   3.3. tenue du registre de la maintenance et des modifications apportées aux services et aux systèmes connexes;
   3.4. surveillance des systèmes de renseignements protégés cotés B et signalement d'accès compromis ou non autorisé par TC aux fonds de renseignements.

4a: SANS CONNEXION À UN RÉSEAU

4a Utilisation d'un poste de travail/ordinateur personnel (PC) autonome:

4a.1 Le poste de travail doit répondre aux exigences de sécurité de base du Centre de la sécurité des télécommunications Canada (CSTC) pour le traitement de données sensibles jusqu'au niveau Protégé B, c.-à-d.:

- 4a.1.1 un produit antivirus reconnu;
- 4a.1.2des produits de réécriture des supports de TI et d'effacement sécurisé approuvés (bulletinB2-002 de la GRC).

4a.2 Le poste de travail ne doit pas être branché à un réseau local (RL) ou intranet (même pendant qu'il n'est pas utilisé pour traiter des données sensibles), ou à Internet.

4a.3Le poste de travail ne doit pas pouvoir être utilisé pour établir une communication sans fil de quelque manière que ce soit (Wi-Fi, modem cellulaire, Bluetooth, etc.).

4a.4 Le nombre de comptes dans le poste de travail doit être limité à un nombre minimal d'utilisateurs autorisés qui détiennent une cote de sécurité valide et appropriée (cela comprend les administrateurs du système et le personnel de soutien).

4a.5 Mots de passe fiables –utiliser un minimum de huit caractères, adopter des règles complexes (caractères alphanumériques, spéciaux, majuscules et minuscules), conserver l'historique des mots de passe, apporter des changements à intervalles réguliers et utiliser des règles de verrouillage.

4a.6 Accès à l'information en fonction du rôle de l'utilisateur –appuyer le principe du «privilège minimal».

4a.7 Expiration de session –fournir un délai raisonnable d'expiration de la session pour les systèmes d'exploitation et les applications.

4a.8 Sécurité du stockage des données –les données inactives doivent être encodées (les produits cryptographiques et les algorithmes doivent être approuvés par le CSTC et être conformes au NIST et au FIPS).

4a.9 Gestion des correctifs et mises à jour de sécurité –appliquer ces mesures rapidement et à intervalle régulier.

4a.10 Gestion de sauvegarde –encoder et conserver les sauvegardes de façon sécuritaire.

4b: AVEC CONNEXION À UNRÉSEAU

4bUtilisez les contrôles techniques et les concepts d'exploitation suivants (s'il y a lieu):

4b.1 Contrôle de l'accès –permet d'éviter tout accès non autorisé. Utiliser des procédures définies pour autoriser, révoquer et surveiller l'accès.

4b.2 Mots de passe fiables –utiliser un minimum de huit caractères, adopter des règles complexes (caractères alphanumériques, spéciaux, majuscules et minuscules), conserver l'historique des mots de passe, apporter des changements à intervalles réguliers et utiliser des règles de verrouillage.

4b.3 Accès à l'information en fonction du rôle de l'utilisateur –appuyer le principe du «privilège minimal».

4b.4 Expiration de session –fournir un délai raisonnable d'expiration de la session pour les systèmes d'exploitation et les applications.

4b.5 Règle d'utilisation du système –définir ce qui constitue une utilisation acceptable et un niveau de sensibilité acceptable de l'information.

4b.6 Sécurité de la communication des données –le transfert de données entre les divers systèmes et les interfaces d'utilisateurs finaux comme IPSec, SSL/TLS(les produits cryptographiques et les algorithmes doivent être approuvés par le Centre de la sécurité des télécommunications Canada (CSTC), le National Institute of Standards and Technology (NIST) et le Federal Information Processing Standard (FIPS).

4b.7 Sécurité du stockage des données –les données inactives doivent être encodées (les produits cryptographiques et les algorithmes doivent être approuvés par le CSTC et être conformes au NIST et au FIPS).

4b.8 Transfert de données sécurisé

4b.8.1 Toute transmission par Internet (courriel) doit être cryptée à l'aide d'une ICP.

4b.8.2 Les données envoyées par la poste doivent être placées dans une enveloppe scellée à usage unique, en indiquant l'adresse de retour, 1reclasse, service Priorité ou courrier recommandé.

4b.8.3 Les supports électroniques envoyés par la poste doivent être cryptés (les produits cryptographiques et les algorithmes doivent être approuvés par le CSTC et être conformes au NIST et au FIPS).

4b.8.4 Le transport de données sensibles doit être fait de manière sécurisée (enveloppe scellée) sans marques de sécurité, avec l'adresse voulue indiquée.

4b.9 Segmentation de réseau pour les serveurs et les bases de données protégés cotés B –utiliser différentes zones de réseau pour séparer les postes de travail des clients, des serveurs d'application et des bases de données au moyen de pare-feu entre les zones et par le filtrage et l'imposition de restrictions d'accès et de circulation.

4b.10 Infrastructure de sécurité –utiliser des pare-feu et des mesures de prévention et de détection des intrusions, des codes malveillants entre les réseaux publics et privés (à la frontière et dans le périmètre du réseau).

4b.11 Enregistrement des activités –suivre de près les accès utilisateur, les registres d'activité (les tentatives de connexion infructueuses).

4b.12 Gestion des correctifs et mises à jour de sécurité –appliquer ces mesures rapidement et à intervalle régulier.

4b.13 Réseautage sans fil –employer une solide authentification et des normes de chiffrage de données.

4b.14 Gestion de sauvegarde –encoder et conserver les sauvegardes de façon sécuritaire.

5. Coter tous les médias électroniques amovibles/externes du niveau de sécurité approprié et sécuriser tous les biens (et renseignements) selon la Politique du gouvernement sur la sécurité.

6. Transfert de données sécurisé

    a. Toute transmission par Internet (courriel) doit être cryptée à l'aide d'une ICP.
    b. Les données envoyées par la poste doivent être placées dans une enveloppe scellée à usage unique, en indiquant l'adresse de retour, 1reclasse, service Priorité ou courrier recommandé.

c. Les supports électroniques envoyés par la poste doivent être cryptés (les produits cryptographiques et les algorithmes doivent être approuvés par le CSTC et être conformes au NIST et au FIPS).
d. Le transport de données sensibles doit être fait de manière sécurisée (enveloppe scellée) sans marques de sécurité, avec l'adresse voulue indiquée.

7. Éliminer toutes les données électroniques qui contiennent ou qui ont contenu des renseignements protégés cotés B, conformément aux exigences du CSTC et de la GRC, lorsque le matériel est remplacé, mis à niveau ou lorsqu'un service est en interruption ou lorsque Transport Canada en fait la demande.

8. Recommandations et pratiques exemplaires:

a. Effectuer des évaluations de la menace et du risque pour les applications et l'infrastructure TI.
b. Mettre en œuvre une politique d'utilisation acceptable du réseau.
c. Établir des normes officielles et des exigences de sécurité de base pour le matériel et les logiciels approuvés.
d. Effectuer périodiquement des évaluations de la vulnérabilité.
e. Utiliser l'authentification à deux facteurs pour les accès administrateur et utilisateur privilégié.
f. Recourir à des pratiques de sécurité exemplaires lors de l'élaboration d'applications personnalisées.
g. Appliquer les pratiques de sécurité exemplaires du fournisseur lors de la configuration du matériel et des logiciels.
h. Appliquer les recommandations du NISTSP-800-53, rév. 3