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

IM/IT Security Classification Guide for defining clearance levels for T8080-200405 – ENHANCING THE CYBERSECURITY READINESS OF CANADA'S ROAD TRANSPORTATION SYSTEM FOR HIGHER LEVELS OF CONNECTIVITY AND AUTOMATION

The following clearance levels are required for the accompanying contract according to the description of the work to be done in the Statement of Work / Terms of Reference supplied to IM/IT Security. The Security Requirements Checklist chosen for this contract offers more than one level of clearance.

Contract Number:	T8080-200405
Contract Title:	ENHANCING THE CYBERSECURITY READINESS OF CANADA'S ROAD TRANSPORTATION SYSTEM FOR HIGHER LEVELS OF CONNECTIVITY AND

Required Clearance Level(s):

Rational for Levels required if more than one level required:

Level	Number Required	Rational
☑ Reliability	3	As and When required. EXAMPLES - *A Reliability level Clearance will be required when Protected levels of information will be accessed on site. Note that no Protected C or Confidential level assets will accessed by the contractor*.
☐ Confidential		
☑ Secret	3	As and when required: EXAMPLES - *A Secret level Clearance will be required when Protected or Classified levels of information will be accessed on site. Note that no Protected C or Confidential level assets will accessed by the contractor*.
☐ Top Secret		

Security Guide for Contractor Sites, Facilities and Information Technology Equipment Producing, Accessing, Storing and/or Processing Protected B Electronic Information

All TC contractors who use their facilities and/or information technology equipment to access, process and/or store sensitive information rated Protected B are required to agree to the following criteria and to provide the required ITS configuration details of their systems and facilities to Transport Canada IM/IT Security.

Requirements:

1. Must permit security inspection and verification of its information technology infrastructure by Transport Canada (TC) if/when required.

2. Employees of Partners or Third Parties:
   2.1. Employees (including contractors) who are granted access to Protected B information or provide administrative, support or maintenance services for the information technology infrastructure and/or its information assets shall possess a valid minimum enhanced reliability security clearance as per Treasury Board Secretariat (TBS) Personnel Screening Standard.

3. Employ the following administrative controls, concepts and risk management philosophies as identified by TBS Operational Security Standard: Management of Information Technology Security (MITS):
   3.1. Change Management and Control processes for approval of changes to software and hardware;
   3.2. Configuration Management – defined and documented;
   3.3. Keep change log records of maintenance and modification to services and associated systems;
   3.4. Monitoring Protected B systems and alerting TC on the compromise, unauthorized access and/or disclosure of information assets originating from TC.

4a: IF NOT CONNECTED TO A NETWORK

4a Employ a standalone workstation / personal computer (PC):

4a.1 The workstation must meet Communications Security Establishment of Canada (CSEC) baseline Security requirements for processing up to Sensitive information at the Protected B level ie.
- 4a.1.1 A proven anti-virus product.
- 4a.1.2 An approved IT Media Overwrite and Secure Erase Product (RCMP Bulletin B2-002).

4a.2 The workstation shall not to be connected to a Local Area Network (LAN) or internet (even when not in use for sensitive activity purposes) or the internet.

4a.3 The workstation shall not have the ability to connect via any form of wireless communication (Wifi, Cellular Modem, Bluetooth, etc)

4a.4 The workstation user accounts shall be limited to a minimum number of authorized users who hold a valid and appropriate level security clearance. (This includes system administrators and support staff)

4a.5 Strong Passwords – minimum 8 characters, complexity rules (alpha numeric, special characters, upper and lower case), employ password history, force change at regular intervals and use lockout rules).

4a.6 Role Based Access to information – in support of the concept of “least privilege”

4a.7 Session Termination – provide a reasonable session timeout delay for operating systems and applications.

4a.8 Secure Data Storage – data at rest must be encrypted. (Cryptographic products and algorithms must be CSEC approved / NIST- FIPS compliant).

4a.9 Patch management and Security updates – applied in a timely manner at regular interval.

4a.10 Backup management – backups are encrypted and securely stored.

4b: IF CONNECTED TO A NETWORK

4b Employ the following technical controls or concepts of operation on networked computers (where applicable):

4b.1 Access Controls – adequate to prevent unauthorized access. Use defined processes and procedures to grant, revoke and monitor access.

4b.2 Strong Passwords – minimum 8 characters, complexity rules (alpha numeric, special characters, upper and lower case), employ password history, force change at regular intervals and use lockout rules).

4b.3 Role Based Access to information – in support of the concept of “least privilege”

4b.4 Session Termination – provide a reasonable session timeout delay for operating systems and applications.

4b.5 System Use Notification – identify acceptable use and the sensitivity level of information

4b.6 Secure Data Communications – data in transit between various systems and all end-user interfaces such as IPSec, SSL /TLS (Cryptographic products and algorithms must be CSEC approved / NIST-FIPS compliant)

4b.7 Secure Data Storage – data at rest must be encrypted. (Cryptographic products and algorithms must be CSEC approved / NIST- FIPS compliant).

4b.8 Secure Data Transfer

4b.8.1 Transmission via internet (email) must be encrypted using PKI.

4b.8.2 Mailing of data to use single sealed envelope, return address, 1st Class Priority Post or Registered Mail

4b.8.3 Electronic media sent by mail must be encrypted (Cryptographic products and algorithms must be CSEC approved / NIST- FIPS compliant).

4b.8.4 Transportation of data outside of Restricted Access Area must be done in secured manner (sealed envelope) with no security markings, appropriately addressed.

4b.9 Network Segmentation for Protected B servers/databases – employ different network zones to separate workstations/clients, application servers and databases by using firewalls between zones and filtering and restricting traffic/access.

4b.10 Security Infrastructure – employ firewalls, intrusion detection/prevention , malicious code detection between private and public networks (at the border / network perimeter)

4b.11 Activity Logging – maintain user access logs and activity logs (unsuccessful login attempts)

4b.12 Patch management and Security updates – applied in a timely manner at regular intervals

4b.13 Wireless Networking – employ strong authentication and data encryption standards.

4b.14 Backup management – backups are encrypted and securely stored.

5. Mark all removable/external electronic media at the appropriate security level and secure assets (and information) according to the Government Security Policy.

6. Secure Data Transfer
    a. Transmission via internet (email) must be encrypted using PKI.
    b. Mailing of data to use single sealed envelope, return address, 1st Class Priority Post or Registered Mail
    c. Electronic media sent by mail must be encrypted (Cryptographic products and algorithms must be CSEC approved / NIST- FIPS compliant).
    d. Transportation of sensitive data must be done in secured manner (sealed envelope) with no security markings, appropriately addressed.

7. Sanitize and dispose of all electronic media which contains or has contained Protected B information according to CSEC and RCMP requirements when hardware is replaced, upgraded, when serviced is discontinued or upon request by Transport Canada.

8. Recommendations and Best Practices:
    a. Perform Threat and Risk Assessments (TRA) for applications and IT infrastructure
    b. Implement a Network Acceptable Use Policy
    c. Establish formal standards and baseline security requirements for approved software and hardware
    d. Perform regular Vulnerability Assessments
    e. Use two-factor authentication for privileged user / administrator access.
    f. Use security best practices when developing custom applications.
    g. Apply vendor security best practices when configuring software and hardware
    h. Apply the recommendations from NIST SP-800-53 Rev.3