AMENDMENT NO. 1

Delete Annex C - Security Requirement checklist (SRCL) and IT Security Safeguard Requirements

Replace with:

ANNEX C – SECURITY REQUIREMENT CHECKLIST AND IT SECURITY SAFEGUARD REQUIREMENTS

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat 1000184378Amended
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: Aboriginal Affairs and Northern Development Canada

2. Branch or Directorate / Direction générale ou Direction: TAG-NW

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

Provide specialized legal translation services from English to French and French to English

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

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) □

Security Classification / Classification de sécurité
UNCLASSIFIED

Canada

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

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

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

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?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
□ No Non ☑ Yes Oui

If Yes, will unscreened personnel be escorted?
Dans l'affirmative, le personnel en question sera-t-il escorté?
☑ No Non □ Yes 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?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?
□ No Non ☑ Yes Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?
☑ No Non □ Yes 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?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?
☑ No Non □ Yes 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?
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?
□ No Non ☑ Yes Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?
☑ No Non □ Yes 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			CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET
											A	B	C			
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).

Aboriginal Affairs and
Northern Development Canada

Affaires autochtones et
Développement du Nord Canada

Aboriginal Affairs and Northern Development Canada

IT Security Safeguard Requirements

Contractor Name	**RFP**
Contract Number	**1000184378**
Document Number:	**9154234**
Date:	**2016-08-30**
Designation / Classification	**Unclassified**

Canada

Overview

In accordance with the Security Requirement Checklist (SRCL) for contract **1000184378**, the contractor will access, store and transmit up to Protected B data. It is the contractor's responsibility to ensure that this information remains secure at all times by complying with the Treasury Board's Policy on Government Security (PGS) (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578), the Management of Information Technology Security Standard (MITS) (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text) and Aboriginal Affairs and Northern Development Canada's (AANDC) Information Security Requirements listed within this document.

Public Works and Government Services Canada (PWGSC) may perform a site inspection to confirm and certify that the contractor meets these requirements. Items of non-compliance will be noted and communicated to the contractor and AANDC for immediate action.

The contractor will be provided a copy of this document and will therefore be aware of these security requirements as well as his or her responsibility to:

- Comply with these requirements;
- Immediately report the loss or theft of any media devices containing AANDC data to AANDC's Departmental Security Officer;
- Notify AANDC's Departmental Security Officer regarding any security breach or suspected security breach which could impact AANDC data; and
- Inform all staff who will be handling AANDC data of these requirements.

Failure to comply with these requirements is a breach of contractual obligations and may result in contract termination.

Possession, Transportation and Processing of Electronic Departmental Data

When there is a requirement for the contractor to transport, process or electronically store departmental information, the contractor must ensure that the data remains secure at all times no matter what level of confidentiality the information is by adhering to the following requirements:

- Computing devices used to process AANDC data are equipped with up to date anti-virus software which is configured to automatically receive and install product updates;
- Computing devices used to process AANDC data must be equipped with up to date software and Operating System versions, and configured to automatically receive and install updates;
- Computing devices are protected by a firewall which can be a network perimeter firewall appliance or host based firewall application installed on the computer (note: a standard router only device is not considered a substitute to a firewall);
- The contractor has the means to securely dispose of electronic data in accordance with CSEC standards (refer to https://www.cse-cst.gc.ca/en/node/270/html/10572);
- Departmental data must be stored on a FIPS 140-2 or above certified removable media device that is encrypted with AES 128 bit algorithm or higher (refer to http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm for a list of certified devices); and
- Portable storage devices must be labeled to indicate the highest classification or designation level of information stored on the device.

Physical Storage of Departmental Data

When there is a requirement for the contractor to store electronic departmental data on their premises, the contractor must ensure that the data remains secure when not in use by adhering to the following requirements:

- The encrypted portable media device(s) must be physically stored within an appropriate security container in accordance with the highest level of information sensitivity that is stored on the device. Such a security container must be present on the contractor's premises (Pro A and B = Padlock security Container / Pro C and Secret Integrated Dial Lock security container - refer to http://www.rcmp-grc.gc.ca/ts-st/reslim/pubs/seg/html/home_e.htm for more information).

Electronic Transmission of Departmental Data

When there is a requirement to electronically transmit departmental data between the contractor and AANDC, the contractor must ensure that only the approved method is used based on the level of sensitivity of the information. The contractor may use a combination of these transmission methods in order to share information with AANDC personnel. The use of electronic transmission methods other than those listed below is prohibited.

Note: The department has Certified and Accredited its remote connectivity services for access to and/or transmission of information up to Protected B. AANDC accepts any residual risk for their use during the contract. Therefore, an IT inspection by PWGSC to verify remote access services is not required.

Classification Level	**AANDC Approved Transmission Methods**	**Requirements**
Protected A	Email	The Contractor can transmit Protected A Data to AANDC personnel via email as long as the following requirements are met: • The e-mail account is not a publically accessible web-mail based service (ex: hotmail, yahoo mail, gmail etc); • Each user has their own corporate e-mail account which is protected with a username and password; and • Email server communication is protected with TLS encryption.
	Fax	The Contractor can transmit Protected A Data to AANDC via fax as long as the following requirements are met: • The sending fax machine is located on the contractor's premises; • The sender contacts the recipient to confirm fax number and advise recipient of incoming fax; • Recipient is present at the fax machine ready to receive fax; and • Sender obtains confirmation from sender of receipt.

	Wireless Communications	If a wireless access point is installed on the contractor’s premises, and devices processing AANDC data will be connected to this network, the wireless infrastructure must at a minimum include the following safeguards: ▪ The administrator user name and password must be changed from their default values; ▪ The network name (SSID) has been changed from its default value; and ▪ WPA2 encryption with an AES algorithm enabled and the passphrase meets the following complexity requirements: • Must be 8 characters or longer; • Have at least one upper case character; • Have at least one lower case character; • Have at least one numeric character; and • Have at least one allowed special character
Protected B	Encrypted and Digitally Signed eMail	The Contractor can transmit Protected B Data to AANDC personnel via email as long as the messages and/or attachments are encrypted and the following requirements are met: • The e-mail account is not a publically accessible web-mail based service (ex: hotmail, yahoo mail, gmail etc); • Each user has their own corporate e-mail account which is protected with a username and password; • The contractor has an approved Public Key Infrastructure (PKI) certificate that is compatible with the Government of Canada (GoC) PKI services; and • Entrust software is installed on the contractor’s PC/laptop and utilized to encrypt the email using the following settings: • One of the following encryption algorithms is used**:** ▪ 3DES-168 Bit or higher ▪ AES-128 Bit or higher • Digitally signed with one of the following algorithms: ▪ RSA (Rivest, Shamir, Adleman) ▪ DSA (Digital Signature Algorithm) ▪ ECDSA (Elliptic Curve Digital Signature Algorithm) • One of the following Hash functions is used in the generation of digital signatures:

		• SHA-224 • SHA-256 • SHA-384 • SHA-512
	Wireless Communications	If a wireless access point is installed on the contractor's premises, and devices processing AANDC data will be connected to this network, the wireless infrastructure must at a minimum include the following safeguards: ▪ The administrator user name and password must be changed from their default values; ▪ The network name (SSID) has been changed from its default value; and ▪ WPA2 encryption with an AES algorithm enabled WPA2 encryption with an AES algorithm enabled and the passphrase meets the following complexity requirements: • Must be 12 characters or longer; • Have at least one upper case character; • Have at least one lower case character; • Have at least one numeric character; and • Have at least one allowed special character
	AANDC Secure File Exchange Service	The Contractor can transmit Protected B Data via AANDC's Secure File Exchange service as long as following requirements are met: • A personally identifiable unique username and password is assigned to the user by AANDC; and • The contractor has read and agrees to abide to the Secure File Exchange Acceptable Use Policy (https://efse-sfee.aadnc-aandc.gc.ca/policy/sfe_Acceptable_use_policy.html)
	AANDC Collaboration Service	The Contractor can transmit Protected B Data via AANDC's Collaboration service as long as following requirements are met: • A personally identifiable unique username and password is assigned to each user by AANDC.

	Fax	The Contractor can transmit Protected B Data to AANDC via fax as long as the following requirements are met: • The sending fax machines is located on the contractor’s premises; • The sender contacts the recipient to confirm fax number and advises recipient of incoming fax; • Recipient is present at the fax machine ready to receive fax; and • Sender obtains confirmation from sender of receipt.