Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8476-226536 002
Security Classification / Classification de sécurité CAN 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	2. Branch or Directorate / Direction générale ou Direction
National Defence	ADM(MAT)/DGLEPM/DSSPM

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

LRF HHTI-LR In Service Support. The scope of this contract provides in-service support for the Laser Range Finder - Hand Held Thermal Imager - Long Range (LRF HHTI-LR) systems in terms of repair and overhaul, supply of spare parts, and the provision of miscellaneous engineering and logistic support.

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) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8476-226536 002
Security Classification / Classification de sécurité CAN UNCLASSIFIED

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

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — [✓] No Non [ ] Yes Oui
   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 :

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

   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? — [ ] No Non [✓] Yes Oui
   Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

   If Yes, will unscreened personnel be escorted? on DND premises, unscreened pers. may only access public/reception zones — [✓] No Non [ ] Yes Oui
   Dans l'affirmative, le personnel en question sera-t-il escorté?

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 Non [✓] Yes Oui
   Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

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

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 Non [✓] Yes Oui
   Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

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 Non [✓] Yes Oui
   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?

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

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	PROTECTED PROTÉGÉ B	PROTECTED PROTÉGÉ 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).

TABLE OF CONTENTS

1. INTRODUCTION 4

2. MANDATORY PREREQUISITES 5

2.1 PSPC VALIDATION 5
2.2 PHYSICAL SECURITY 5
2.3 PERSONNEL SECURITY 9
2.4 PROCEDURAL SECURITY 9
2.5 INFORMATION SECURITY 10

3. MINIMUM IT SECURITY REQUIREMENTS 13

3.1 IT SECURITY POLICY COMPLIANCE AND MONITORING 13
3.2 IT SYSTEM CONFIGURATION 13
3.3 IT EQUIPMENT 15
3.4 AUTHORIZATION AND ACCESS CONTROL 16
3.5 IT MEDIA 18
3.6 DOCUMENT PRINTING AND/OR REPRODUCTION 19
3.7 RECOVERY 20
3.8 DISPOSAL 20

1. INTRODUCTION

1.1 The IT Security Requirements Document. This "IT Security Requirements Document for Contract W8476-226536 002 is being provided in accordance with the instructions for completion of Part C, Section 11.d of the Treasury Board Secretariat (TBS) Form 350-103 which states:

"Will the supplier be required to use its IT systems to electronically process and/or produce or store PROTECTED and/or CLASSIFIED information and/or data? If Yes,. . . The client department and/or organization will be required to specify the IT security requirements for this procurement in a separate technical document. . ."

Each IT Security Requirements Document applies only to the contract for which it is written. Accordingly this "IT Security Requirements Document for Contract W8476-226536 002 is specific to Contract W8476-226536 002.

1.2 DND's IT Security Requirements. This document outlines the Department of National Defence's (DND) Information Technology (IT) security requirements for the electronic storage / processing / creation of this contract's Proprietary Information up to and including the level of PROTECTED B, as applicable to Controlled Technical Data.

1.3 Proprietary Information. The term "Proprietary Information" is defined - for this document only - as any government assets and/or Sensitive (Designated or Classified) information which is stored / processed / created by private organizations to fulfil a contract with DND where contract security is administered by the Public Services and Procurement Canada Contract Security Program (PSPC/CSP).

1.4 Connectivity Criteria for IT Link. In the event that the Information System (IS) used to electronically store / process / create this Proprietary Information is also required to electronically connect to DND's infrastructure (i.e. the Security Requirements Check List (SRCL) Part C, Section 11.e is checked as "YES"), a separate IT Link "Connectivity Criteria" document will be completed by the Project Officer (PO) for the DND Project Management Office (PMO), and this link will require validation and authorization from PSPC/CSP.

1.5 Layers of Security Protection. Security is based upon layers of protection; in order for IT security requirements to effectively safeguard information they must be preceded and supported by other aspects of security and their associated policies. Contracting efforts should be preceded by the implementation of physical, personnel, procedural, information, and IT security safeguards.

1.6 Additional Information. The Contract Security Manual (CSM), available from Public Services and Procurement Canada (PSPC), prescribes the procedures to be applied by Canadian-based organizations for the safeguarding of government information and assets. Additional security information is available on the internet from PSPC/CSP, as well as the Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (CCCS), and the Royal Canadian Mounted Police (RCMP).

2. MANDATORY PREREQUISITES

2.1 PSPC Validation

2.1.1 Contract Security Manual (CSM). The contractor must ensure that, for the duration of the contract, all applicable security requirements in the CSM as well as all security requirements in this document are met. Whenever there are two requirements for the same issue, the most stringent requirement must be applied.

2.1.2 Contractor Sites. The contractor must inform PSPC/CSP and the DND PO of all physical sites where this contract's Controlled Technical Data Proprietary Information will be stored / processed / created. This includes any applicable main and/or alternate contractor offices, construction sites, back-up storage locations, partners, all levels of sub-contractors offices, etc.

2.1.3 Site Requirements. Every site used to electronically store / process / create this contract's Proprietary Information must be granted a Facility Security Clearance (FSC) as well as either a Designated Organization Screening (DOS) or a Document Safeguarding Capability (DSC), as applicable. Every site must also be cleared by PSPC/CSP prior to being authorized to electronically store / process / create Proprietary Information.

2.2 Physical Security

2.2.1 Facility Authorization. Storage / processing / creation of this contract's Proprietary Information must only be performed in facilities which have been authorized by the PSPC/CSP. All data must be stored / processed / created in a secure manner that prevents unauthorized viewing, access, or manipulation.

2.2.2 Physical Security Zones. In accordance with the RCMP's "*G1-026 Guide to the Application of Physical Security Zones*", the IS - identified herein for this document only as the LRF HHTI-LR IS - will be installed and operating in an Operations Zone or in a temporary Operations Zone.

2.2.3 Proprietary Information Outside of Canada. Storage / processing / creation of Proprietary Information outside of Canada is, under the following conditions, authorized under this contract.

2.2.3.1 The foreign contractor must first be evaluated and authorized by PSPC/CSP and the DND PO.

2.2.3.2 Per Section 9.8 of the CSM, when awarding contracts, including subcontracts, to organizations outside of Canada holding a valid facility security clearance (FSC) in their nation (foreign contractor), organizations are required to get the Canadian DSA approval for the contract and/or sub-contract.

2.2.4.5 Any issues inside Canada concerning the PSPC/CSP will be handled outside of Canada by Canadian Designated Security Authority (Canadian DSA).

2.2.4 Mobile Computing/Teleworking. Mobile computing/teleworking (MC-TW) involving the IS or Proprietary Information is, under the following conditions, authorized under this contract.

2.2.4.1 PSPC/CSP must first authorize and, when determined by PSPC/CSP, inspect the MC-TW site.

2.2.4.2 the contract's CSO must notify the DND PO as well as PSPC/CSP of any security violation, significant incident or compromise concerning MC-TW.

2.2.4.3 All aspects of MC-TW must abide by all applicable IT security requirements in this document.

2.2.4.4 CSO Responsibilities Prior to MC-TW. The following information is to be documented and made available, upon request, to the DND PO. Prior to any employee starting MC-TW, the CSO or ACSO must:

2.2.4.4.1 approve in writing each Contractor employee's MC-TW;

2.2.4.4.2 verify that the MC-TW employee holds a valid personnel security screening which has been granted by PSPC/CSP; this security screening must be - at minimum - a Reliability Status;

2.2.4.4.3 verify that the employee has attended an IT security awareness training session/briefing, as required by the "IT Security Awareness Training" para of the "IT Security Requirements Document for Contract W8476-226536 002;

2.2.4.4.4 verify that the MC-TW employee has read the system-specific IT Security Orders and signed a related User Agreement form, as required by the "User Agreement Form" para of the "IT Security Requirements Document for Contract W8476-226536 002; and this User Agreement must include requirements and restrictions concerning MC-TW;

2.2.4.4.5 verify that the physical location(s) where the MC-TW will take place (e.g. the MC-TW employee will be working from his/her residence or from another location), the location(s) must be assessed for risk in the context of Temporary Operations Zone security requirements, in accordance with the Annex B and C of the Contract Security Manual (CSM) Contract Security Manual – Security requirements for contracting with the Government of Canada - Security screening - National security - National Security and Defence – Canada.ca (tpsgc-pwgsc.gc.ca);and

2.2.4.4.6 verify that, if applicable and required to use WI-FI when working remotely, the MC-TW employee must follow CCCS's "ITSAP.80.009 - Protecting Your Organization While Using Wi-Fi".

2.2.4.5 Contractor Responsibilities. The Contractor:

2.2.4.5.1 must provide each employee with Contractor-owned/leased IT equipment and the software required for the contract; anti-virus/anti-malware software, a Contractor-managed operating system as well as a reputable FIPS 140.2 or 140-3 compliant storage/hard drive encryption tools (e.g. Bitlocker, VeraCrypt, etc.) must be installed using separate administrator credentials under Contractor's IT team's control; the IT equipment must not contain generic, guest, temporary, or shared accounts of any kind;

2.2.4.5.2 must ensure that the IT equipment is set-up to only use secure remote-access or virtual private network (VPN) technologies with modern encryption protocols (such as TLS 1.3, or IKEv2) in accordance with the CCCS "ITSP.40.062 - Guidance on Securely Configuring Network Protocols" and the CCCS "ITSP.40.111 -

Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information".

2.2.4.5.3 must ensure, if the MC-TW employee does not have the means to securely store the MC-TW equipment when not in use, that the Contractor provides these means to the MC-TW employee for his/her remote place(s) of work; and

2.2.4.5.4 must provide Contractor-owned removable IT media to any MC-TW employee, if the use of removable IT media (e.g. USB sticks, CDs/DVDs, etc.) is allowed under this contract.

2.2.4.5.5 The Prime contractor must ensure that all applicable employees and any subcontractor employee hired to work on part of the contract adhere to all the MC-TW's requirements (normally through signature of an updated Acceptable-Use-Policy for IT equipment).

2.2.4.6 MC-TW Employees - Responsibilities. While using the MC-TW IT equipment, the MC-TW employee:

2.2.4.6.1 must stop working immediately and contact his/her CSO or ACSO if the security requirements in this document cannot be met or if the MC-TW employee is aware of any security violation, significant incident, or compromise of Proprietary Information;

2.2.4.6.2 must ensure that when not in use, all MC-TW IT equipment and any authorized removable storage media is stored securely, as stated in the CSM. The Contractor must ensure that, if the MC-TW employee does not have the tools and/or means for securely storing (when not in use) the IT equipment and any authorized removable storage media, the Contractor provide these tools to the MC-TW employee for his/her remote place(s) of work.

2.2.4.6.3 is not authorized to store / process / create Proprietary Information on his/her personally-owned IT equipment or removal IT media;

2.2.4.6.4 is not authorized to store / process / create / send / receive emails containing Proprietary Information via Contractor-provided smart phone unless specifically authorized in writing by the DND PO;

2.2.4.6.5 is not authorized to connect the MC-TW IT equipment to any public, unencrypted or open Wi-Fi;

2.2.4.6.6 must ensure that encryption on personal Wi-Fi used for MC-TW is kept current with GC standards and must remain current during the entire period of MC-TW; and

2.2.4.6.7 must - if use of removable IT media is authorized - use only removable IT media provided by the Contractor.

2.2.4.7 Contractors and MC-TW Employees - Responsibilities.

2.2.4.7.1 When using MC-TW, the MC-TW IT equipment:

2.2.4.7.1.1 must ensure that firmware patches/updates for the supported anti-virus/anti-malware application,

operating systems and other applications installed on the MC-TW device are updated regularly and kept current;

2.2.4.7.1.2 should use multi-factor authentication for connections between the MC-TW device and the contractor's network, per CCCS publication "Secure Your Accounts and Devices with Multi-Factor Authentication (ITSAP.30.030)"; and

2.2.4.7.1.3 must follow guidelines in CCCS's "Annex 2 - Wireless User to Wired Network Connection High-Level Design Guidance (ITSG-41)". Additional recommendations are available in CCCS's "Protecting your Organization While Using WI-FI (ITSAP.80.009)" and "Virtual Private Networks (ITSAP.80.101)".

2.2.4.7.2 When using MC-TW to process Proprietary Information the IT media (e.g. removable media, internal hard drives, etc.) must be encrypted using the most current GC approved encryption technology for the sensitivity level of the information being processed; and the encryption used must be kept current for the length of the contract. Information on encryption is available in "Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111)".

2.2.4.7.3 When using MC-TW the Contactor and the Contractor employee must review and follow the recommendations in CCCS's "Security Tips for Organizations With Remote Workers (ITSAP.10.016)" and "Cyber Security Tips for Remote Work (ITSAP.10.116)".

2.2.4.8 MC-TW and MC-TW Employees - Information Required. Details on the following, which are to be provided to the DND PO upon request, must be documented by the Contractor for each MC-TW employee:

2.2.4.8.1 the highest sensitivity level of data to be processed by the MC-TW employee, which must be no higher than Protected B;

2.2.4.8.2 the type of IT equipment to be used. For example thin client (a dumb terminal unit); or fat client (PC, laptop, tablet, etc.);

2.2.4.8.3 the type of account to be used for the remote work (e.g. normal user, privilege accounts or group membership, etc.);

2.2.4.8.4 how the Proprietary Information is to be uploaded to/downloaded from the IT equipment (e.g. VPN connection or - if authorized - removable media (e.g. USB sticks, CDs/DVDs, etc.);

2.2.4.8.5 type of encryption used for the hard drive(s) and removable media, and/or password protection for the individual data files. This should include the type and level of encryption to be used and the method of accessing the VPN;

2.2.4.8.6 the physical location(s) where the MC-TW will take place (e.g. the MC-TW employee will be working from his/her residence or from another location); and

2.2.4.8.7 the following information on all IT devices that each MC-TW employee will be using for MC-TW: the type and number of devices, make, model, and year of manufacture.

When using MC-TW the Contactor and the Contractor employee must review and follow the recommendations in CCCS publications "Security Tips for Organizations With Remote Workers (ITSAP.10.016)" and "Cyber Security Tips for Remote Work (ITSAP.10.116)".

2.3 Personnel Security

2.3.1 Security Screening Level of Personnel. All contractor personnel who have access to any Proprietary Information must:

2.3.1.1 hold - at minimum - a valid RELIABILITY STATUS which must be granted and be tracked by PSPC/CSP; and

2.3.1.2 be assigned system privileges on the criteria of least privilege; this means applying the most restrictive set of privileges and the need-to-know principle (i.e. limiting access to information only to those whose duties require such access) necessary for the performance of authorized tasks; and

2.3.2 Access to the Physical Security Zone. No visitors, foreign nationals or unauthorized personnel shall have access to the Proprietary Information, the LRF HHTI-LR IS, or the zone where the Proprietary Information is being stored / processed / created unless they possess a valid RELIABILITY STATUS and are escorted by an authorized contractor employee.

2.3.3 IT Security Awareness Training. All contractor personnel handling Proprietary Information must be provided training and/or briefing sessions coordinated and delivered by the CSO or the ACSO. This training must, at minimum, make reference to the PSPC "Contract Security Manual" (CSM) and other security information as determined by the DND PO, as well as the system-specific IT Security Orders and Standard Operating Procedures (SOP) for the LRF HHTI-LR IS. Training should also cover social engineering, use of social media, and situational awareness.

2.4 Procedural Security

2.4.1 IT Security Orders and Standard Operating Procedures. The contractor must create system-specific IT Security Orders for IS as well as SOPs relating to the operation and maintenance of the LRF HHTI-LR IS. This SOP should be kept up to date and should be made available to authorized personnel who have a functional requirement to review and/or revise the document. These documents must - at minimum - address:

2.4.1.1 roles and responsibilities (e.g. CSO, technical authority, IS system administrator(s), etc.);

2.4.1.2 access management for the Operations Zone and the LRF HHTI-LR IS;

2.4.1.3 acceptable use policy for the LRF HHTI-LR IS;

2.4.1.4 identify the frequency and the method used to update the operating system (OS) security patches and provide details on the OS configuration;

2.4.1.5 details on IT incident management procedures;

2.4.1.6 identify the frequency and the method used to update the anti-virus definition files as well as the configuration of the anti-virus/anti-malware application;

2.4.1.7 include a list of every installed application and its version as well as the application patch management process;

2.4.1.8 identify the frequency and the method used to review OS log files as well as the personnel tasked with reviewing the OS log files;

2.4.1.9 must include an Authorization and Access Control process depicting the user addition and removal process (details are available in "User Authentication Guidance for Information Technology Systems (ITSP.30.031 v3)";

2.4.1.10 include details on the back-ups (e.g. frequency, methodology, storage, etc.).

2.4.1.11 any other subject identified in this document; and

2.4.1.12 any other issue(s) identified by the DND PO or the DND PMO during the life of this contract.

2.4.2 User Agreement Form. All personnel having access to the IS must read the system-specific IT Security Orders for the LRF HHTI-LR IS and sign an associated User Agreement Form, as produced and tracked by the CSO or ACSO. All changes to the system-specific IT Security Orders, SOPs and/or User Agreement Form must be promulgated to all personnel having access to the IS.

2.4.3 System Administrator - Personnel Security Screening Level. The IS must be administered and maintained internally by individual(s) possessing - at minimum - a valid SECRET (lvl ll) Clearance.

2.4.4 Vulnerability Management and Incident Reporting. Per Annex A, Section VI of the CSM, a vulnerability management process must be identified and followed to ensure risks from vulnerabilities are managed. The contractor must also report any security incident to the DND Project Lead by no later than 24 hours after it has been detected or reported to PSPC.

2.4.5 IS Continuous Monitoring. The contractor must continually monitor its overall security posture including physical, personnel, procedural, information, and IT security. The contractor must inform PSPC/CSP and the DND PO of any issues that could potentially impact the security of the Proprietary Information or the IS.

2.5 Information Security

2.5.1 Document Marking. All documents - hardcopy (paper) and softcopy (electronic) - containing Proprietary Information must be marked with the highest security level of the information contained in the document, and be afforded a unique identifier to ensure positive control and tracking.

2.5.2 Information at Rest. The contractor must protect the security of the Proprietary Information at rest through physical and/or IT security measures.

2.5.2.1 When unattended, all hardcopy (paper) documents containing Proprietary Information (e.g. paper printouts, etc.) and all removable IT media used to store / process / create Proprietary Information must be physically locked in Government of Canada (GC) approved security container(s) appropriate to the

information's sensitivity level. The container(s) must be in accordance with the RCMP's "G1-001 Security Equipment Guide"; as this Guide is not available to the general public, the contractor can contact the DND PO for information.

2.5.2.2 When unattended all removable IT media used to store / process / create Proprietary Information must be encrypted using GC-approved encryption technology appropriate for the sensitivity level of the Proprietary Information it contains. This is to protect the information in case the IT media is lost, misplaced or stolen.

2.5.2.3 Only contractor personnel authorized to have access to the Proprietary Information will be given the means to unencrypt electronic documents and/or have access to the key(s) and/or combination(s) for the approved secure container(s) used to store the information.

2.5.3 Exchange of Proprietary Information. When exchanging Proprietary Information between DND and all levels of contractors/sub-contractors, all hard copy documents and IT media must be handled and transported/transmitted in accordance with GC guidelines as stated in the CSM or the RCMP's "*G1-009 Transport and Transmittal of Protected and Classified Information*". When transported (i.e. hand carried from one person/place to another by an individual who has the need-to-know and is screened to the highest level of the Proprietary Information) or transmitted (i.e. sent from one person/place to another by a third party), all electronic media must be encrypted using GC-approved encryption technology for the sensitivity level of the information contained in the electronic media.

2.5.4 Exchange of Proprietary Information - Packaging. All hard copy documents and IT media must be packaged appropriately and transported/transmitted with a covering letter as well as a transmittal form or circulation slip which must indicate:

2.5.4.1 the highest sensitivity level of information contained in the package;

2.5.4.2 the date of transport/transmission;

2.5.4.3 the unique identifier for each document/IT media in the package;

2.5.4.4 the printed name and phone number of the originator;

2.5.4.5 the signature of the originator;

2.5.4.6 the physical street address of the destination;

2.5.4.7 the printed name and phone number of the recipient; and

2.5.4.8 the signature of the recipient.

2.5.5 Segregation of Proprietary Information for Emergency Destruction. All Proprietary Information (e.g. hard copy documents, IT media, etc.) must be segregated from other contractual and corporate information in a way that allows all Proprietary Information to be securely destroyed or wiped immediately, upon request from PSPC/CSP or the DND PO as indicated in the CSE publication "*IT Media Sanitization (ITSP.40.006)*".

2.5.6 Controlled Goods. Contracts involving Controlled Goods must treat their information electronically as PROTECTED B, at a minimum, and contact the Controlled Technology and Transfer (CTAT) section at CTATProgramandCompliance-ATTCProgrammeetConformite@forces.gc.ca for additional security requirements.

2.5.7 Sub-contractors. The contractor must inform the DND PO and officially register with PSPC/CSP any partners and all levels of partnership and sub-contractors involved in

this contract. The contractor is ultimately responsible for ensuring that all security requirements and all relevant and/or associated security documentation relating to this contract are provided to the contractor's partners and all levels of sub-contractors.

2.5.8 IT Security Requirements for Sub-Contracts. All applicable IT security requirements in this contract must also be included in any sub-contracts.

3. MINIMUM IT SECURITY REQUIREMENTS

3.1 IT Security Policy Compliance and Monitoring

3.1.1 Compliance and Monitoring. On a frequency and schedule to be determined by the DND IT Security Authority, DND retains the right to conduct inspections of any contractor facility involved in this contract to ensure compliance with the IT Security requirements herein as well as compliance with GC standards and policies concerning the prevention, detection, response, and recovery requirements.

3.2 IT System Configuration

3.2.1 Basic system configuration. The basic system configuration is anticipated by the DND PO to be a network of servers, workstations (PCs, laptops, or tablets), printers/MFDs, and scanners. This network could be a segment of one of the contractor's existing networks or an entirely new network. Removable media (e.g. CDs/DVDs, USB sticks, etc.) may be used for uploading/downloading information. This network could have connectivity to the internet.

3.2.2 Network Security. If the IS is configured as a network, the contractor must implement perimeter defence and network security safeguards (e.g. firewalls, etc.) for the IS to negotiate all traffic and to protect servers and IT equipment that is externally accessible.

3.2.3 Segregation of IS. If configured as a segment of one of the contractor's existing networks, the contractor must segregate the networks into IT security zones and implement perimeter defence and network security safeguards. CSE and CCCS provide guidelines on this specific subject; see "*Network Security Zoning - Design Considerations for Placement of Services within Zones (ITSG-38)*" and "*Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)*". Details on segregation methodology (i.e. topology diagram and other documents as deemed necessary) must be provided to PSPC/CSP and the DND PO for evaluation.

3.2.4 Type of Equipment. The equipment used to store / process / create the Proprietary Information must consist of Commercial Off The Shelf (COTS).
All equipment must be labelled commensurate with the highest sensitivity level of Proprietary Information to be processed on the equipment. Examples of processing equipment for this IS could include workstations (PCs, laptops, tablets), servers, IT storage devices (network-attached storage (NAS), storage area network (SAN)), printers, scanners, etc.

3.2.5 IS Hard Drives. Processing equipment can be configured with internal, removable and / or external hard drives.

3.2.6 Operating System(s). All applicable IT equipment used for the LRF HHTI-LR IS must operate on supported Operating Systems (OS); i.e. the vendor of each OS must be creating and providing current security patches for the OS. OS security patches must be installed regularly, at least monthly. The OS must be hardened; i.e. unnecessary processes, services, ports, etc. must be disabled. The IS SOP must provide details on the OS configuration and must identify the frequency and the method used to update the OS security patches.

3.2.7 Anti-virus/Anti-malware Software. A supported anti-virus/anti-malware application must be installed and operating on all applicable IT equipment. Anti-virus/anti-malware definition files must be updated regularly - at least daily. The IS SOP must identify the frequency and the method used to update the anti-virus/anti-malware

definition files as well as the configuration of the anti-virus application. Configuration of the anti-virus/anti-malware application must:

3.2.7.1 allow changes to be made only by the system administrator(s);

3.2.7.2 automatically scan all applicable LRF HHTI-LR IS IT equipment at power-on or on a set interval, at least weekly; and

3.2.7.3 scan every new file introduced to the LRF HHTI-LR IS for malicious code.

3.2.8 Software and Applications. Only applications required under this contract must be installed on the IS. Application patches must be kept up-to-date and be managed through a defined configuration management process. The IS SOP must list every installed application and its version, as well as identify the application patch management process. The following are the minimum IT Security Requirements/Recommendations for the web-based (HTTPS) access to a single-sign-on Collaborative Environment (CE) to exchange only up to Protected B contract's DND/CAF Proprietary Information:

3.2.8.1 Website must use Secure Hypertext Transfer Protocol (HTTPS) for secure communication (encrypted) with the most recent Transport Layer Security (TLS) protocol such as; TLS 1.2 or 1.3. For securing web services, follow guidelines set forth in NIST SP 800-95 and guidelines for web services encryption, follow the guidelines set forth in NIST SP 800-175A, SP 800-175B Rev.1, FIPS 140-2 and FIPS 186-4;

3.2.8.2 Schedule website security audits to identify and address vulnerabilities, we recommend that the web application has security measures implemented to prevent the most top10 (OWASP) critical security concerns such as; Injection, Broken authentication, Sensitive data exposure, XML external entities (XXE), Broken access control, Security misconfigurations, Cross site scripting (XSS),Insecure deserialization, Using components with known vulnerabilities; and Insufficient logging and monitoring;

3.2.8.3 Update your website or software regularly;

3.2.8.4 Install security plugins and make sure they are updated;

3.2.8.5 Use automatic back-up for your website;

3.2.8.6 Establish a password authentication or a public/private key for authentication;

3.2.8.7 Enforce strong passwords and change them regularly;

3.2.8.8 Deploy two-factor authentication to access the website;

3.2.8.9 Create levels of access, limit access to the specific parts of the website they need to use to complete their day to day tasks, least privilege;

3.2.8.10 Deploy a Web application firewall (WAF);

3.2.8.11 Choose a web hosting provider that offers 24/7/365 network monitoring and firewall protection to block any known threats

3.2.8.12 Use best practices for Secure Software Development Framework (SSDF) to mitigate the risk of Software Vulnerabilities according to NIST's white paper publication https://doi.org/10.6028/NIST.CSWP.04232020 (CSWP.04232020); and

3.2.8.13 Appropriate certifications and/or accreditations for compliance must be obtained if the web applications and APIs will be processing sensitive data such as financial (PCI DSS), healthcare (HIPAA), and PII (Personally Identifiable Information) to make sure they are protected (encrypted) when in use, in transit and as well as at rest.

3.2.10 Logging and Auditing. OS logging must be active and the system administrator(s) for the LRF HHTI-LR IS must ensure that the logs are reviewed at least quarterly or whenever there has been a suspected compromise. The logging and review must consist of - but not be limited to - successful logins; unsuccessful login attempts; unauthorized changes to the system hardware, firmware, and software; unusual system behaviour; unplanned disruption(s) of systems and/or services; system errors; etc. Only the system administrator(s) shall be allowed to modify or delete log files and only after being authorized by the CSO or ACSO. The IS SOP must identify the frequency and the method used to review the OS log files.

3.3 IT Equipment

3.3.1 Equipment Inventory. A list of all equipment forming the IS must be maintained by the contractor. This equipment list must contain - at minimum - the equipment's description, make, model, and quantity. If requested, this equipment list must be made available to PSPC/CSP and the DND PO.

3.3.2 Changes to IT Equipment. The contractor must inform PSPC/CSP and the DND PO of any major change(s) to the LRF HHTI-LR IS IT equipment.

3.3.3 Bluetooth Technology. The use of Bluetooth technology as part of the system's IT equipment is strictly prohibited. The use of Bluetooth technology in the Operations Zone or the temporary Operations Zone where the IS is located is strictly prohibited except in the case of approved medical devices; the CSO must be advised of any Bluetooth medical device that is used in the proximity of the LRF HHTI-LR IS and must authorize the use of this device in writing.

3.3.4 Wi-Fi or Wireless. The use of Wi-Fi or wireless capabilities as part of the IS is authorized under the following conditions:

3.3.4.1 Wi-Fi/wireless requirements for contractor employees working remotely (i.e. MC TW employees) are covered in Section 2 above under the "Mobile Computing/ Teleworking" subsection.

3.3.4.2 Wi-Fi/wireless capabilities can be used at the Contractor's site(s) under the following conditions:

3.3.4.2.1 Any Wi-Fi/wireless connection to the IS must be protected by encryption. The use of WPA2 protocol is suggested; minimum encryption of 128-bit is mandatory, 256-bit encryption is highly encouraged.

3.3.4.2.2 The contractor must establish usage restrictions including access enforcement mechanisms; only authorized personnel will be given accounts on the Wi-Fi/wireless connection.

3.3.4.2.3 Best practices as outlined in CCCS publication "Annex 2 - Wireless User to Wired Network Connection High-Level Design Guidance (ITSG-41)" must be followed.

3.3.4.2.4 Modification of Wi-Fi/wireless settings is not authorized at the user level; any modifications are to be done only by the system administrator(s) and only after written agreement from the DND PO.

3.3.4.2.5 Any Wi-Fi/wireless capabilities used to store / process / create Proprietary Information at the Contractor's site(s) must first be validated, inspected and authorized by PSPC/CSP.

3.3.5 Cloud Technology. The use of public or third party “cloud” technology to store / process / create Proprietary Information is authorized under the following conditions:

3.3.5.1 The contractor is only authorized to use Canada Post Connect.

3.3.6 Network Interconnectivity. All network equipment interconnectivity:

3.3.6.1 can use CAT 6 cable or wireless/Wi-Fi to connect the IS equipment;

3.3.6.2 must be identifiable from any other system wiring;

3.3.6.3 must be controlled and monitored to prevent inadvertent or deliberate connection to any unauthorized equipment, network or infrastructure; and

3.3.6.4 can be installed in standard corporate wiring infrastructure.

3.3.7 Topology Diagram. A topology diagram of the LRF HHTI-LR IS must be provided, upon request, to PSPC/CSP and/or the DND PO. The diagram must consist of a high-level system design and include any IT links to other entities and/or connections to other networks and/or systems, where applicable.

3.3.8 IT Equipment Maintenance and Disposal. Maintenance and disposal of any IT equipment used to store / process / create Proprietary Information (e.g. workstations, servers, printers, plotters, scanners, photocopiers and/or Multi-Function Devices (MFDs)/Multi-Function Printer (MFPs), etc.) must follow the instructions provided in the “Disposal” section, below.

3.4 Authorization and Access Control

3.4.1 List of Authorized Personnel. The contractor must maintain a list of authorized individuals who have access to the IS. This list must be updated whenever there is a change of personnel or a change to an individual's information that is contained on the list. The list must include, at minimum:

3.4.1.1 the individual's name

3.4.1.2 the individual's approved clearance level;

3.4.1.3 the date the individual's clearance expires; and

3.4.1.4 the type of account (e.g. user, power user, event log reader, administrator, etc.).

3.4.2 System Accounts.

3.4.2.1 An individual Administrator account must be created for each system administrator. If an individual requires both administrator access and regular user access, the individual must have two separate accounts on the IS. Administrator accounts must not be used for standard day-to-day operations or non-administrative issues.

3.4.2.2 An individual User account must be created for each user; each account must have a unique name/identifier, and this name/identifier cannot be used by any other account holder for the life of the system. User accounts must be configured for limited privileges and must allow access only to the files and folders required by the user to perform their specific duties.

3.4.2.3 The IS must not contain:

3.4.2.3.1 any generic accounts,

3.4.2.3.2 any guest accounts,

3.4.2.3.3 any temporary accounts, or

3.4.2.3.4 shared accounts of any kind.

3.4.3 Passwords.

3.4.3.1 Each account must be protected by a password with an enforced minimum password complexity, as follows:

3.4.3.1.1 the password must contain a minimum of eight (8) characters;

3.4.3.1.2 the password must contain three of the following four criteria:

- at least one uppercase letter (A through Z),
- at least one lowercase letter (a through z),
- at least one number (0 through 9), and
- at least one special character (e.g. !, $, #, %, etc.);

3.4.3.1.3 password lifetime restrictions: minimum of one day and maximum of 90 days;

3.4.3.1.4 password reuse is prohibited for the previous ten (10) passwords; and

3.4.3.1.5 the account must lock after four (4) consecutive failed logon attempts.

3.4.3.2 Any password used to access the IS:

3.4.3.2.1 must be changed at first login;

3.4.3.2.2 must be changed whenever there is any suspicion of compromise;

3.4.3.2.3 must not be the same as that user's password for any other Contract W8476-226536 002 IS;

3.4.3.2.4 must not be saved or remembered by the OS or any application accessed by the OS; and

3.4.3.2.5 must never be shared with anyone.

3.4.3.3 The original local administrator password on all IT equipment forming the IS must be changed; vendor default passwords must not be used. Each time a local administrator password is changed it must be promulgated to all applicable personnel (e.g. IT support, system administrators, etc.) who must safeguard it commensurate with the highest sensitivity level of data processed on the system. It should be written down and placed in a sealed envelope which has been signed and dated over the flap by the CSO, ACSO or system administrator. The envelope must be locked in an approved container and safeguarded commensurate with the highest sensitivity level of data processed on the system for which the password is used.

3.4.4 IS Access Control List. All network elements (physical and/or virtual) of the IS must be tracked and be accessible (e.g. via access control list (ACL), Active Directory, etc.) only to authorized personnel.

3.4.5 Authorization and Access Control in SOP. The IS SOP must include an Authorization and Access Control process depicting the procedures for adding, disabling, and deleting user accounts.

3.5 IT Media

3.5.1 Disposal of IT Media. Throughout the duration of this contract, all IT media used to store / process / create Proprietary Information must be disposed of in accordance with the “Disposal” section of this document.

3.5.2 Removal of IT Media. In the event that equipment requires maintenance, support or replacement, **no IT media containing any Proprietary Information** (e.g. internal hard drives, removable IT media, etc.) will be given or made available to any outside vendor, service provider or other unauthorized personnel.

3.5.3 Identification of IT Media. All IT media (e.g. internal hard drives, removable hard drives, external hard drives, CDs/DVDs, USB sticks, etc.) used to store / process / create Proprietary Information must:

3.5.3.1 be dedicated to this contract only;

3.5.3.2 be given a unique identifier to ensure positive control and tracking;

3.5.3.3 be identified and inventoried by:

3.5.3.3.1 the type of media (e.g. CD/DVD, USB stick, etc.),

3.5.3.3.2 the information sensitivity level,

3.5.3.3.3 the release-ability caveat (if applicable),

3.5.3.3.4 the model and serial number (if applicable), and

3.5.3.3.5 the IT media's unique identifier;

3.5.3.4 be labelled with:

3.5.3.4.1 the highest sensitivity level of the data it contains,

3.5.3.4.2 the government department (in this case DND),

3.5.3.4.3 the contract number, and

3.5.3.4.4 the IT media's unique identifier.

3.5.3.5 If a label cannot be affixed directly on the IT media, the label must be attached to the IT media by other means (e.g. string, etc.).

3.5.4 Safeguarding of IT Media. All IT media must be safeguarded commensurate with the highest sensitivity level of the data it contains. When not being used all removable IT media - including failed, life cycled and long-term use media (e.g. backup media, etc.) - must be locked in a secure container approved to the information sensitivity level of the data that it contains.

3.5.5 Logging of Removable IT Media. The location of all removable IT media must be tracked and controlled via the use of a log book. The log book must contain, at minimum:

3.5.5.1 the type of media (e.g. CD/DVD, USB stick, removable hard drive, backup tape, etc.);

3.5.5.2 the IT media's unique identifier;

3.5.5.3 the date and time it was removed from its GC-approved security container;

3.5.5.4 the name, or initials, and signature of the individual who signed it out;

3.5.5.5 the date and time it was returned to its GC-approved security container; and

3.5.5.6 the name, or initials, and signature of the individual who returned the media.

3.5.6 Air Gap Computer. The LRF HHTI-LR IS is not required to interact with untrusted sources (e.g. the internet, another network, removable IT media from another source, etc.) that would require the contractor to provide a standalone Air Gap computer.

3.6 Document Printing and/or Reproduction

3.6.1 Printing/Reproduction Authorization. The contractor is:

3.6.1.1 authorized to print and/or reproduce any Proprietary Information within the contractor’s premises; and

3.6.1.2 authorized to use external printing and/or reproduction services.

Use of either of these services to print and/or reproduce any Proprietary Information must first be approved by PSPC/CSP and the DND PO.

3.6.2 Printing/Reproduction Device Hard Drives. Devices used to reproduce Proprietary Information (e.g. printers, plotters, scanners, photocopiers, MFDs/MFPs, etc.) can be equipped with internal and / or removable hard drives.

3.6.3 Printer Connections. Unless the IS is configured as a segment of the contractor's corporate network, all printers, plotters, scanners, photocopiers and/or MFDs/MFPs must only be connected to the IS. Connection to other devices or networks is strictly prohibited.

3.6.4 Connection of Telephone Lines. The connection of telephone lines to any MFD/MFP used to process Proprietary Information is strictly prohibited.

3.6.5 Reproduction of Particularly Sensitive Information. For any extremely sensitive Proprietary Information, printing/reproduction of each document must first be approved by the DND PO; and if approved, every copy must be afforded a unique identifier to ensure positive control and tracking.

3.7 Recovery

3.7.1 IS Backups. The Proprietary Information must be backed up regularly, at least once a week; and the backups must be safeguarded at a remote location (i.e. a different location unlikely to be affected by the same incident, such as a fire or flood, which could affect the primary location). If the contractor does not have a remote location to safeguard the backups, arrangements can be made with the DND PO. If backups are to be safeguarded by a private organization other than the contractor, this must be addressed though a sub-contract. The IS SOP must include details on the back-up frequency, methodology and storage.

3.7.2 Testing of Backups. The IS backups should be tested on a regular basis. The IS SOPs should include details on the back-up testing frequency, methodology and reporting of errors.

3.7.3 Disaster Recovery Plan. The contractor must develop, and document a Disaster Recovery Plan (DRP) for the IS. This DRP must include details on the recovery, restoration, testing frequency, and methodology.

3.8 Disposal

3.8.1 Authorization for Disposal. The disposal of all IT media used for this contract - including removable media, internal and external hard drives - must be authorized in advance by the DND PO and must be documented and tracked. This includes for example, IT media that has failed, is being life cycled, is no longer required, etc. If hard drives cannot be removed from devices used to store / process / create Proprietary Information (e.g. tablets, etc.) then the devices must be returned to the DND PO.

3.8.2 On-Site Disposal. On-site disposal at the contractor's facility of any IT media used to store / process / create Proprietary Information is authorized under the following conditions:

3.8.2.1 the contractor must possess equipment that has been approved for the destruction of PROTECTED B, as applicable to Controlled Technical Data information per the RCMP's "G1-001 Security Equipment Guide";

3.8.2.2 the contractor must destroy of all IT media in accordance with CSE publication "IT Media Sanitization (ITSP.40.006)"; and

3.8.2.3 if the contractor does not have the required disposal means, arrangements must be made with the DND PO for disposal of IT media.

If disposal of IT media is prohibited at the contractor's site the contractor must make arrangements for disposal with the DND PO.

3.8.3 Disposal of IT Media - Tracking. The disposal of IT media must be tracked via the use of a "Certificate of Destruction" (if applicable) and a "Transit and Receipt Form"; the DND PO will provide templates for these documents. The contractor must retain a copy of all IT disposal documents as evidence that the IT media has been properly disposed of. The contractor must:

3.8.3.1 forward a copy of these documents to PSPC/CSP by email at 'tpsgc.dgsssiprojetintl-dobissintlproject.pwgsc@tpsgc-pwgsc.gc.ca'; and

3.8.3.2 provide a copy of these documents to the DND PO/PMO upon request.

3.8.4 Return of All Proprietary Information. At the end of the contract all Proprietary Information (hard copies and electronic) must be returned to the DND PO. This includes all paper copies of documents as well as any IT media used to store / process / create Proprietary Information (e.g. internal hard drives (used in workstations, laptops, servers, photocopiers, MFDs/MFPs, etc.); CDs/DVDs; USB sticks; SD cards; external hard drives; etc.). If hard drives cannot be removed from devices used to store / process / create Proprietary Information (e.g. tablets, etc.) then the devices must be returned to the DND PO.

3.8.5 Procedures Prior to Removal of IT Equipment. If maintenance and/or disposal of IT equipment is necessary, the following procedures must be applied prior to removing any IT equipment used to store / process / create Proprietary Information; this process applies to all IT equipment containing IT media (e.g. servers, workstations, printers, plotters, scanners, MFDs/MFPs, etc.):

3.8.5.1 All non-volatile memory devices (internal, removable, and external hard drives, etc.) must be removed and be disposed of as indicated in this section.

3.8.5.2 Volatile memory (e.g. RAM, DRAM, SRAM, etc.) must be sanitized by removing all power for a minimum of 24 consecutive hours. The contractor must ensure there is no power to the memory (e.g. from internal batteries or through connection to another device). If there is any doubt concerning the removal of all power to volatile memory in equipment used to store / process / create highly sensitive Proprietary Information, the contractor must remove the volatile memory from the device and have it destroyed.

3.8.5.3 Any stickers or security markings on the device - in connection with this contract or the IS - must be removed.

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:
PWGSC FILE No. W8476-226536-002

1. The Contractor must, at all times during the performance of the Contract, hold a valid Designated Organization Screening (DOS), and obtain approved Document Safeguarding and Production Capabilities at the level of PROTECTED B, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

2. This contract includes access to **Controlled Goods.** Prior to access, the contractor must be registered in the Controlled Goods Program of Public Works and Government Services Canada (PWGSC).

3. The Contractor personnel requiring access to PROTECTED information, assets, or sensitive site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CSP, PWGSC.

4. The Contractor MUST NOT utilize its facilities to process, produce, or store PROTECTED information or assets until the CSP, PWGSC has issued written approval.

5. The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce, or store PROTECTED information until the CSP, PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED B.

6. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the CSP, PWGSC.

7. The Contractor must comply with the provisions of the:

   (a) Security Requirements Check List and security guide (if applicable), attached at Annex D2;
   (b) *Contract Security Manual* (Latest Edition)