Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution

Electronics, Simulators and Defence Systems Div.
/Division des systèmes électroniques et des systèmes de simulation et de défense
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Title - Sujet Remote Minehunting and Disposal Sys Système de détection et d'élimination des mines sous-marines	
Solicitation No. - N° de l'invitation W8472-105270/C	**Amendment No. - N° modif.** 002
Client Reference No. - N° de référence du client W8472-105270	**Date** 2021-09-21
GETS Reference No. - N° de référence de SEAG PW-$$QF-125-28275	
File No. - N° de dossier 125qf.W8472-105270	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à** 02:00 PM Eastern Daylight Saving Time EDT **on - le** 2021-11-10 Heure Avancée de l'Est HAE	
F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☑	
Address Enquiries to: - Adresser toutes questions à: Lacoursiere, Paul	**Buyer Id - Id de l'acheteur** 125qf
Telephone No. - N° de téléphone (343) 551-1529 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature** **Date**	

Canada

This Request for Proposal (RFP) Amendment # 002 for the Remote Minehunting and Disposal System (RMDS) is raised to:

1. Provide answers to Industry questions;
2. Make updates to the solicitation documentation.

1. Please see the below questions with responses:

Question 10,

Given that the proposed solution must be COTS and/or MilCOTS, we expect that our equipment provider will be a supplier (not a subcontractor) to our company. Would Canada please confirm that we may propose an FSR provided by a bidder's supplier?

Response 10,

No. The Field Service Representative (FSR) provided for evaluation is expected to be the same resource available to provide FSR services through the In-Service Support (ISS) contract.

Question 11,

In Volume 1, paragraph 3.1 specifies Section IV: Addition Information but in paragraph 3.1.5 specifies Section IV: Value Proposition Proposal. Can Canada provide clarification?

Response 11,

Yes. Volume 1 will be amended to specify Section IV: Value Proposition Proposal and Section V: Additional Information.

Question 12,

We respectfully request Canada to agree to cap the contractor's liability for damages to Canada to a mutually agreed specific dollar amount that is no greater than the value of the contract. Paragraph 7.15 Volume 2 contains a heading, Limitation of Liability, but without any text below it.

Response 12,

Canada will follow the stated Standard Acquisition Clauses and Conditions (SACC) Manual 2030 (2020-05-28), General Conditions - Higher Complexity – Goods. Para 7.15 and header will be removed.

Question 13,

Can Canada please confirm that Volume 2, Annex A, Appendix 1 paragraph 3.2.3.8 should read, "The Lightweight AUV should have ..."

Response 13,

Yes. See amendment to Volume 2, Annex A, Appendix 1 paragraph 3.2.3.8.

Question 14,

The Mechanical Shock requirements in accordance with D-03-003-007/SG-000 Grade 1 Type A outlined in Section 7.2 of the System Requirements Document (Volume 2, Annex A, Appendix 1) implies a Heavy Weight shock qualification at a certified test facility using the Floating Shock Platform. Should the costs and schedule impacts be reflected in each bidder’s proposal?

Response 14,

Yes. It is required that all costs and schedule associated with environmental testing and qualification be included in the bidder's proposal.

Question 15,

Can Canada clarify what level of personnel security screening level is required?

Response 15,

Personnel security screening level of SECRET is required. Please see amendments to Volume 2 and 3, Annex C.

Question 16,

Would Canada please confirm whether Proprietary Information which is not PROTECTED and/or CLASSIFIED information or data' is subject to the requirements in the 'Information Technology Security Requirements Document'?

Response 16,

No, it is not. Only PROTECTED and/or CLASSIFIED information is subject to the "Information Security Requirements Document".

Question 17,

As one or more of the main RMDS subsystems may be sourced from a company(ies) who do not have offices in Canada, would Canada reconsider requirement 2.2.4 of the 'Information Technology Security Requirements Document'?

Response 17,

The requirement has been updated. Please see amendments to Volume 2 and 3, Annex C.

Question 18,

Can Canada clarify the term "Designated" in the ‘Information Technology Security Requirements Document'?

Response 18,

"Designated" consists off all levels of "PROTECTED".

Question 19,

We respectfully request Canada to agree to cap the contractor's liability for damages to Canada to a mutually agreed specific dollar amount that is no greater than the value of the contract. Paragraph 7.16 of volume 3 contains a heading, Limitation of Liability, but without any text below it.

Response 19,

Canada will follow the stated Standard Acquisition Clauses and Conditions (SACC) Manual 2035 (2018-06-21), General Conditions - Higher Complexity – Services. Para 7.16 and header will be removed.

Question 20,

Section 11c of Part A of the SRCL for In-Service Support (ISS), states that there will be no production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occurs at the supplier's site or premises.

Can Canada clarify this requirement as it is expected that equipment for the remote minehunting disposal system (RMDS) may need to be repaired and/or modified at the Contractor's site as part of the ISS contract?

Response 20,

Proposals may or may not include PROTECTED and/or CLASSIFIED equipment. If equipment or components in the bidder’s proposal are determined to be of a sensitive nature (PROTECTED and/or CLASSIFIED), the SCRL and Contract security clauses will need to be amended, including level of Document Safeguarding Capability (DSC), and demonstrated to be met prior to the contract award.

2. Please see the following changes to the solicitation documents.

8, At Volume 1, paragraph 3.1

Delete: The bid must be gathered per section and separated as follows:

Section I: Technical Bid
Section II: Financial Bid
Section III: Certifications
Section IV: Additional Information

Insert: The bid must be gathered per section and separated as follows:

Section I: Technical Bid
Section II: Financial Bid
Section III: Certifications
Section IV: Value Proposition Proposal
Section V: Additional Information

9, At Volume 1, paragraph 6.1 (e)

Delete: Para (e) the Bidder must provide the addresses of proposed sites or premiseses of work performance and document safeguarding as indicated in Part 3-section IV Additional information.

Insert: Para (e) the Bidder must provide the addresses of proposed sites or premiseses of work performance and document safeguarding as indicated in Part 3-section V Additional information.

10, At Volume 2, paragraph 7.15

Delete: complete paragraph 7.15

11, At Volume 2, Annex A, Appendix 1, paragraph 3.2.3.8;

Delete: complete paragraph
Insert: The Light Weight AUV should have a coverage rate in detection only mode of at least 0.40 km^2/hr or more in a type A1 bottom while meeting the minimum sonar resolution.

12, At Volume 2, Annex C;

Delete: complete Annex C
Insert: Volume 2, Annex C

ANNEX C

Security Requirements Check List

Remote Minehunting and Disposal System (RMDS)

(Electronic copy available from the Contracting Authority)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8472-105270 Amendment 2
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 Organizati Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: DGMEPM/MSC
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

The work required delivery of the Remote Minehunting and Disposal System. The effort includes delivery of all subsystems, integration into a containerized solution and delivery of integrated logistics support including technical documentation and training.

	No / Non	Yes / Oui
5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?		✓
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?	✓	
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)		✓
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.	✓	
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?	✓	

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
W8472-105270 Amendment 2
Security Classification / Classification de sécurité
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? ✓ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

On DND premises, unscreened pers. may only access public/reception zones

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?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8472-105270 Amendment 2
Security Classification / Classification de sécurité
Unclassified

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).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8472-105270 Amendment 2
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	
Shawn Beaudette	MSC 7-2	BEAUDETTE, SHAWN 529	Digitally signed by BEAUDETTE, SHAWN 529 Date: 2020.12.01 12:26:14 -05'00'

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-762-7039		Shawn.Beaudette@forces.gc.ca	2021-08-17

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sasa Medjovic	Senior security analyst	MEDJOVIC SASHA 234	Digitally signed by MEDJOVIC, SASHA 234 DN: C=CA, O=GC, OU=DND-MDN, OU=Personnel, OU=INTERN, CN="MEDJOVIC, SASHA 234" Reason: I am the author of this document Location: your signing location here Date: 2021.08.20 13:37:13-04'00' Foxit PhantomPDF Version: 10.1.4

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-996-0286		sasa.medjovic@forces.gc.ca	

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
Paul Lacoursiere	Supply Team Lead; Navigation, Sonar and Radar Systrems	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
343-551-1529		Paul.Lacoursiere@	

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
C. Jason Quade Contract Security Officer Jason.Quade@pwgsc-tpsgc.gc.ca		

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

ANNEX C

Appendix 1

Department of National Defence (DND)

Information Technology Security Requirements Document

for

Contract W8472-105270 AMENDMENT 1

RELEASE HISTORY

VERSION	AMENDMENT DATE	AMENDMENT DETAILS	AMENDED BY
1.0	2021-03-25	Initial draft	Capt Martineau DIM Secur
1.1	2021-03-31	Final Version	Julie Bastarache, DIM Secur
1.2	2021-08-13	Amendment 2, paragraph 2.2.4	Shawn Beaudette, DGMEPM
1.3	2021-08-17	Accepted the proposed amendment to para 2.2.4. Final Version	Rob Kabano, DIM Secur

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The IT Security Requirements Document. This "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1 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 it is written for; accordingly this "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1 is specific to Contract W8472-105270 AMENDMENT 1.

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 CONFIDENTIAL and NATO CONFIDENTIAL.

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. . As per the SOW and its annexes, the Shared Data Environment (SDE) used by the Contractor must be solely for unclassified data and it is forbidden to store, process, create or transmit classified data, protected data or Controlled Goods.

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 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). All well as the security requirements in the CSM, the additional requirements stated in this document must be 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 CONFIDENTIAL and NATO CONFIDENTIAL 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.

2.1.4 Emanation Security (EMSEC). As this contract has been evaluated at the CONFIDENTIAL and NATO CONFIDENTIAL level, the contractor is required to conform to Emanation Security (EMSEC) specifications as depicted in the CSE/CCCS "*Emission Security (EMSEC) Guidance (ITSG-11A)*". This publication can be obtained from PSPC/CSP or the DND PO.

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 W8472-105270 AMENDMENT 1 IS - will be installed and operating in a Security zone.

2.2.3 Physical Security Zone - Access Control List. Access to the security zone will be controlled by an Access Control List (ACL); a copy of the ACL will be affixed inside the security zone where the IS is installed and operating. This ACL will be updated by the Company Security Officer (CSO) or the Alternate Company Security Officer (ACSO) whenever there is a change of personnel who are authorized to access this area.

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

2.2.4.1 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.

2.2.4.2 The foreign contractor must follow all conditions set out in the "IT Security Requirements Document for Contract W8472-105270" and the "Air Gap Computer Document for Contract W8472-105270".

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

2.2.4.4 If unable to adhere to all security requirements, the foreign contractor is required to provide “proposed mitigation measures against specific requirements” which will be reviewed by the DND PO and then discussed with the foreign contractor to determine safeguards acceptable to DND.

2.2.5 Mobile Computing/Teleworking. Mobile computing/teleworking (MC-TW) for contractor employees working from home which involves the IS or Proprietary Information is not authorized for this contract.

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 Secret (Level II) Security Clearance which must be granted and be tracked by PSPC/CSP;

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 W8472-105270 AMENDMENT 1 IS, or the zone where the Proprietary Information is being stored / processed / created unless they possess a valid Secret (Level II) Security Clearance and are escorted by an authorized contractor employee. An audit log must be maintained of all visitors, foreign nationals or unauthorized personnel accessing the security zone.

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 W8472-105270 AMENDMENT 1 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 W8472-105270 AMENDMENT 1 IS. 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 security zone and the IS;

2.4.1.3 acceptable use of the IS;

2.4.1.4 incident management procedures;

2.4.1.5 any other subject identified in this document and

2.4.1.6 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 W8472-105270 AMENDMENT 1 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 valid Secret (Level II) Security Clearance

2.4.4 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).

2.5.3 Exchange of Proprietary Information. When exchanging Proprietary Information between DND and all levels of contractors/sub-contractors via hard copy and/or removable IT media, all hard copy documents and removable IT media must be handled and transported/transmitted in accordance with GC guidelines as depicted 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 encryption technology approved 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 CCCS publication "*IT Media Sanitization (ITSP.40.006)*".

2.5.6 Controlled Goods. For this contract, the contractor will require access to Confidential and NATO Confidential and Controlled Goods information or equipment.

2.5.6.1 All GC Controlled Goods data (hard and soft copy) must be marked in accordance with DND Defence Administrative Orders and Directives (DAOD) 3003-1. The contractor must abide by all GC Controlled Goods regulations including Controlled Technology Access and Transfer (CTAT) and International Traffic in Arms Regulations (ITAR), where applicable. Additional information can be obtained from the *Controlled Goods Regulations (SOR/2001-32)* (https://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-32/), the DND CTAT office through the DND PO, or the PSPC Controlled Goods Program by email to dmc-cgd@tpsgc-pwgsc.gc.ca.

2.5.6.2 If any Controlled Goods regulations differ from the Information Technology Security Requirements in this document, the most stringent regulation/requirement is to be applied.

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

On a frequency and schedule to be determined by the DND IT Security Authority, DND retains the right to conduct inspections of every contractor's 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 Type of System. The IS must be configured as standalone system.

3.2.2 Type of Equipment. The equipment used to store / process / create the Proprietary Information must consist of Commercial Off The Shelf (COTS) if within a certified EMSEC zone otherwise TEMPEST equipment must be used; and must be labelled commensurate with the highest sensitivity level of Proprietary Information to be processed on the equipment.

3.2.3 IS Hard Drives. Processing equipment must be configured with removable hard drives. Examples of processing equipment for this IS include workstations (PCs, laptops, tablets), servers, IT storage devices (network-attached storage (NAS), storage area network (SAN)), printers, scanners, etc.

3.2.4 Operating System. The IS must operate on a supported Operating System (OS); i.e. the vendor of the 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 configured to disable unnecessary processes, services, and ports. The IS SOP must provide details on the OS configuration and identify the frequency and the method used to update the OS security patches.

3.2.5 Anti-virus/Anti-malware Software. A supported anti-virus/anti-malware application must be installed and operating on all workstations and servers (as applicable). Anti-virus/anti-malware definition files must be updated regularly and kept current. The IS SOP must provide details on the configuration of the anti-virus/anti-malware application as well as identify the frequency and the method used to update the anti-virus/anti-malware definition files. Configuration of the anti-virus/anti-malware application must:

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

3.2.5.2 automatically scan all W8472-105270 AMENDMENT 1 IS workstations/servers at power-on or on a set interval, at least weekly; and

3.2.5.3 scan every new file introduced to the IS workstations/servers for malicious code.

3.2.6 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.

3.2.7 Logging and Auditing. OS logging must be active and the log files must be reviewed by the W8472-105270 AMENDMENT 1 IS system administrator(s) at least monthly. The 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 W8472-105270 AMENDMENT 1 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 security zone or the temporary security zone where the IS is located is strictly prohibited except in the case of approved medical devices; the CSO must be advised of all Bluetooth medical devices that are used in the proximity of the W8472-105270 AMENDMENT 1 IS.

3.3.4 Wireless or Wi-Fi. The use of wireless or Wi-Fi capabilities on the IS is strictly prohibited.

3.3.5 Cloud Technology. The use of a public or third party "cloud" to store / process / create Proprietary Information is strictly prohibited

3.3.6 Topology Diagram. A topology diagram of the W8472-105270 AMENDMENT 1 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.

3.3.7 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 access (e.g. user, power user, 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. !, $, #, %);

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 must:

3.4.3.2.1 be changed at first login;

3.4.3.2.2 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 W8472-105270 AMENDMENT 1 IS;

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

3.4.3.2.5 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 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.

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 Air Gap Computer. If the IS is required to interact with untrusted sources (e.g. the internet, another network, removable IT media from another source, etc.) the contractor will be required to provide a standalone Air Gap computer. Data transfer security requirements and related instructions for the Air Gap computer will be provided by the DND PO in a separate technical document; a template for this is available from DIM Secur upon request.

3.5.6 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:

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

3.5.6.2 the IT media's unique identifier;

3.5.6.3 the date and time it was removed;

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

3.5.6.5 the date and time it was returned; and

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

3.6 Personal IT Devices (PITDs)

3.6.1 The contractor must ensure that all Personal IT Devices (e.g. cell phones, smart watches, fit bits, etc.) are kept outside the security zone where the W8472-105270 AMENDMENT 1 IS is located.

3.7 Document Printing and/or Reproduction

3.7.1 Printing/Reproduction Authorization. The contractor is:

3.7.1.1 authorized to print and/or reproduce any Proprietary Information within the contractor’s premises using local printing device attached to the IS via tempest cable or fiber optic cable; and

3.7.1.2 not 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 and authorized by PSPC/CSP and the DND PO.

3.7.2 Printing/Reproduction Device Hard Drives. Devices used to reproduce Proprietary Information (e.g. printers, plotters, scanners, photocopiers, MFDs/MFPs, etc.) must be equipped with removable hard drives. If a device does not support removable hard drives a different device, with no hard drive or with a removable hard drive, must be used.

3.7.3 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.

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

3.7.5 Reproduction of Particularly Sensitive Information. For any particularly 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.

3.8 Recovery

3.8.1 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. another building). 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.

3.8.2 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.

3.8.3 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.

3.9 Disposal

3.9.1 Authorization for Disposal. The disposal of all IT media used on 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.

3.9.2 On-Site Disposal. On-site disposal at the contractor's facility of any IT media used to store / process / create Proprietary Information is strictly prohibited.

3.9.3 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 make these IT disposal documents available to PSPC/CSP and the DND PO upon request.

3.9.4 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. Due to the use of control goods by the contractor, the assets with control goods must be demilitarised in coordination with the DND PO.

3.9.5 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.):

3.9.5.1 Any device used to print PC or Classified Proprietary Information on this contract:

3.9.5.1.1 must print at least 50 copies of a page completely filled with unclassified text; this is in order to remove any possible data remaining on the drums, belts or other internal components of the device; and

3.9.5.1.2 must dispose of all toner cartridges by the same method used for disposal of IT media that has failed, is being life cycled, or is no longer required. This disposal is to prevent security incidents from toner cartridges which contain built-in drums and could retain images of printed documents.

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

3.9.5.3 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.

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

Department of National Defence (DND)

Air Gap Computer Document

for

Contract W8472-105270 AMENDMENT 1

RELEASE HISTORY

VERSION	AMENDMENT DATE	AMENDMENT DETAILS	AMENDED BY
1.0	2021-03-25	Initial draft	Capt Martineau, DIM Secur
1.1	2021-03-31	Final Review and Conversion from sister contract W8482-206387	Julie Bastarache, DIM Secur

TABLE OF CONTENTS

1. INTRODUCTION

1.1 This document outlines the Information Technology (IT) security requirements for Department of National Defence (DND) Contract W8472-105270 AMENDMENT 1 for the transfer of electronic information between the Information System (IS) - identified herein for this document only as the W8472-105270 AMENDMENT 1 IS - used to store / process / create this contract's Proprietary Information up to and including the level of CONFIDENTIAL or NATO CONFIDENTIAL. The scope of this "Air Gap Computer Document for Contract W8472-105270 AMENDMENT 1" is to state the minimum IT security requirements necessary to transfer electronic information to and from the IS.

1.2 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).

1.3 As this contract may require data inputs from untrusted sources, there is a need for an additional level of IT security to mitigate the possibility of infection or malware originating from untrusted sources. These extra steps are intended to protect not only the W8472-105270 AMENDMENT 1 IS but also any other system exchanging information with the IS. The transfer of all Proprietary Information into the IS will be required to transition through an Air Gap Computer.

1.4 The application of the IT security safeguards listed in this document are based on the mandatory requirement that the physical premises have been inspected, assessed and authorized to store / process / create information up to and including CONFIDENTIAL or NATO CONFIDENTIAL. Validation must be provided by PSPC/CSP.

2. MANDATORY PREREQUISITES

2.1 Description

2.1.1 A standalone workstation (i.e. PC or laptop) equipped with a removable hard drive as well as two approved and supported anti-virus/anti-malware applications must be used for all electronic data transfers into the IS. The transfer of electronic data into this IS is allowed only from a system of equivalent sensitivity level or lower.

2.1.2 The transfer of electronic data from the W8472-105270 AMENDMENT 1 IS must first be authorized in writing by the DND Project Officer (PO).

2.2 Terminology

2.2.1 The following terminology will be used in this document.

Source File	The data to be transferred to the Target System; the Source File must not have a higher sensitivity level than the Target System.
Source System	The IS that the Source File came from.
Target System	The IS that the Source File will be uploaded to. The Target System is the W8472-105270 AMENDMENT 1 IS.
Source Transfer Media	The removable electronic media (e.g. CDs/DVDs, USB sticks, SD cards, external hard drives, etc.) containing the Source File from the Source System. For the W8472-105270 AMENDMENT 1 IS the type(s) of Source Transfer Media will be DVD only.
Target Transfer Media	The removable electronic media to be used to move the Source File from the W8472-105270 AMENDMENT 1 Air Gap Computer to the Target System. For the W8472-105270 AMENDMENT 1 IS the type(s) of Target Transfer Media will be DVD only.,

2.3 Hardware

2.3.1 This Air Gap Computer must be located in the same physical security zone as the Contract W8472-105270 AMENDMENT 1 IS and use the same type of equipment (e.g. COTS or TEMPEST) as stated in section "Type of Equipment" of the "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1".

2.3.2 For the entire length of the contract, this Air Gap Computer must be used <u>only</u> for this purpose.

2.3.3 This Air Gap Computer must be owned by the contractor and be installed, configured, and operational before being inspected by PSPC/CSP.

2.3.4 This Air Gap Computer must consist, preferably, of a stand-alone PC with only a monitor, keyboard and mouse or, alternately, a laptop. No other peripheral equipment (e.g. printer, scanner, etc.) can be attached to the Air Gap Computer.

2.3.5 If using a PC, the Air Gap Computer must be equipped with a removable hard drive.

2.3.6 This Air Gap Computer must be installed and operating in the same security zone zone where the W8472-105270 AMENDMENT 1 IS is installed.

2.3.7 Labelling. This Air Gap Computer and removable hard drive (if applicable) must be affixed with a label identifying the highest sensitivity level of the contract's Proprietary Information which is being transferred using this equipment.

2.3.8 Labelling of Transfer Media. The Transfer Media to be used on this Air Gap Computer must be marked with the following information:

2.3.8.1 the highest sensitivity level of the data it contains,

2.3.8.2 the government department (in this case DND),

2.3.8.3 the contract number (in this case W8472-105270 AMENDMENT 1),

2.3.8.4 the IT media's unique identifier, as discussed in para 3.5.3.2 of the "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1", and

2.3.8.5 the transfer media category (either "Source Transfer Media" or "Target Transfer Media").

2.3.9 If this information cannot be written directly on the media or if a large label (approximately 4" by 6") cannot be affixed directly on the media, the label must be attached to the IT media by other means (e.g. string, etc.).

2.3.10 The "Source Transfer Media" and the "Target Transfer Media" should be labelled with different colours (e.g. black for one, red for the other) to easily differentiate between them.

Figure 1: example labels

2.4 IT System Configuration

2.4.1 This Air Gap Computer must operate on a supported Operating System (OS) and must follow all items specified in the paragraph "Operating System" of the "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1". As well as disabling unnecessary processes, services, and ports, all unnecessary computer components (e.g. network card, microphone, speakers, etc.) must also be disabled.

2.4.2 Two different anti-virus/anti-malware applications must be installed on this contract's Air Gap Computer and these applications must be supported. This contract's Air Gap Computer must follow all items specified in the paragraph "Anti-virus/Anti-malware Software" of the "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1".

2.4.3 Any other applications installed on this contract's Air Gap Computer shall be deleted/uninstalled, and no other applications can be installed on this computer.

2.4.4 OS logging must be active on this contact's Air Gap Computer, and all items specified in the paragraph "Logging and Auditing" of the "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1" must be followed.

2.4.5 All accounts on this contact's Air Gap Computer must follow the applicable sections of the paragraph "Authorization and Access Control" of the "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1". No shared or generic accounts are authorized.

2.4.6 The following paragraphs of the "IT Security Requirements Document for Contract W8472-105270 AMENDMENT 1" are applicable to this Air Gap Computer and must be followed:

- "Unattended Removable Media";
- "IT Media";
- "Personal IT Devices (PITDs)"; and
- "Disposal".

2.5 Air Gap Computer and SOP

2.5.1 The W8472-105270 AMENDMENT 1 IS SOP must include the procedures and details mentioned in this "Air Gap Computer Document for Contract W8472-105270 AMENDMENT 1" for all applicable aspects of this Air Gap Computer.

3. DATA TRANSFER PROCEDURES

3.1 The following process must be used to transfer electronic data from any untrusted source(s) to the IS.

3.2 These Data Transfer Procedures must be posted near the W8472-105270 AMENDMENT 1 Air Gap Computer.

DATA TRANSFER PROCEDURES

1. Power on the W8472-105270 AMENDMENT 1 Air Gap Computer and logon.
2. Ensure that the definition files for both anti-virus/anti-malware applications are current. If not current, update the necessary definition files before proceeding.
3. Copy the Source File(s) from the Source System to the Source Transfer Media. If the Source File(s) is/are already on removable electronic media (e.g. removable media received from a vendor, etc.), then this can be used as the Source Transfer Media.
4. Label the Source Transfer Media and connect it to the Air Gap Computer.
5. Scan the Source Transfer Media and all Source File(s) using both anti-virus/anti-malware applications.
   a. If any viruses/malware are detected, STOP the procedure. Clean/delete the file(s) as directed by the anti-virus/anti-malware applications and inform the Company Security Officer (CSO) or the Alternate Company Security Officer (ACSO).
   b. If no viruses/malware are detected, proceed to the next step.
6. Copy the Source File(s) from the Source Transfer Media onto the Air Gap Computer.
7. Remove the Source Transfer Media from the Air Gap Computer.
8. Label the Target Transfer Media and connect it to the Air Gap Computer.
9. Copy the scanned Source File(s) from the Air Gap Computer to the Target Transfer Media.
10. Remove the Target Transfer Media from the Air Gap Computer.
11. Connect the Target Transfer Media to the Target System.
12. Copy the scanned Source File(s) from the Target Transfer Media to the Target System.
13. Ensure that the scanned Source File(s) copied to the Target System can be opened and are not corrupted.
14. If the Source File(s) on the Target System is/are satisfactory:
    a. delete the Source File(s) from the Target Transfer Media;
    b. remove the Target Transfer Media from the Target System; and
    c. delete the Source File(s) from the Air Gap Computer.
15. Log off and shut down the Air Gap Computer.

13, At Volume 3, paragraph 7.16

Delete: complete paragraph 7.16

14, At Volume 3, Annex C;

Delete: complete Annex C
Insert: Volume 3, Annex C

ANNEX C

Security Requirements Check List

Remote Minehunting and Disposal System (RMDS)

(Electronic version is available from the Contracting Authority)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8482-206387 Amendment 2
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 Organizati Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM (Mat) / DGMEPM / MSC
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

The work requires the provide the in-service support to the Remote Minehunting and Disposal System (RMDS). This effort includes repair and maintenance of the RMDS at the contractor facility and DND sites, engineering services including field service representatives, maintenance of publicationsa and technical data, sparing support and project management.

	No / Non	Yes / Oui
5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?		✓
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?	✓	
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)		✓
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.	✓	
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?	✓	

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
W8482-206387 Amendment 2
Security Classification / Classification de sécurité
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 : Remark on 10 b) On DND premises, unscreen personnel may only access public, reception zones

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? ✓ 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).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8482-206387 Amendment 2
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	
Shawn Beaudette	MSC 7-2	BEAUDETTE, SHAWN 529	Digitally signed by BEAUDETTE, SHAWN 529 Date: 2020.12.01 12:26:14 -05'00'

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-762-7039		Shawn.Beaudette@forces.gc.ca	2021-08-17

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sasa Medjovic	Senior security analyst	MEDJOVIC, SASHA 234	Digitally signed by MEDJOVIC, SASHA 234 DN: C=CA, O=GC, OU=DND-MDN, OU=Personnel, OU=INTERN, CN="MEDJOVIC, SASHA 234" Reason: I am the author of this document Location: your signing location here Date: 2021.08.20 13:50:46-04'00' Foxit PhantomPDF Version: 10.1.4

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-996-0286		sasa.medjovic@forces.gc.ca	

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	
Paul Lacoursiere	Supply Team Lead; Navigation, Sonar and Radar Systrems		

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
343-551-1529		Paul.Lacoursiere@	

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
C. Jason Quade Contract Security Officer Jason.Quade@pwgsc-tpsgc.gc.ca			

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

ANNEX C

Appendix 1

Department of National Defence (DND)

Information Technology Security Requirements Document

for

Contract W8482-206387

RELEASE HISTORY

VERSION	AMENDMENT DATE	AMENDMENT DETAILS	AMENDED BY
1.0	2021-03-25	Initial draft	Capt Martineau DIM Secur
1.1	2021-03-26	Final Version	Julie Bastarache
1.2	2021-08-13	Amendment 2, paragraph 2.2.4	Shawn Beaudette, DGMEPM
1.3	2021-08-17	Accepted the proposed amendment to para 2.2.4. Final Version	Rob Kabano, DIM Secur

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The IT Security Requirements Document. This "IT Security Requirements Document for Contract W8482-206387 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 it is written for; accordingly this "IT Security Requirements Document for Contract W8482-206387 is specific to Contract W8482-206387.

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 CONFIDENTIAL and NATO CONFIDENTIAL.

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. . As per the SOW and its annexes, the Shared Data Environment (SDE) used by the Contractor must be solely for unclassified data and it is forbidden to store, process, create or transmit classified data, protected data or Controlled Goods.

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 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). All well as the security requirements in the CSM, the additional requirements stated in this document must be 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 CONFIDENTIAL and NATO CONFIDENTIAL 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.

2.1.4 Emanation Security (EMSEC). As this contract has been evaluated at the CONFIDENTIAL and NATO CONFIDENTIAL level, the contractor is required to conform to Emanation Security (EMSEC) specifications as depicted in the CSE/CCCS "*Emission Security (EMSEC) Guidance (ITSG-11A)*". This publication can be obtained from PSPC/CSP or the DND PO.

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 W8482-206387 IS - will be installed and operating in a Security zone.

2.2.3 Physical Security Zone - Access Control List. Access to the security zone will be controlled by an Access Control List (ACL); a copy of the ACL will be affixed inside the security zone where the IS is installed and operating. This ACL will be updated by the Company Security Officer (CSO) or the Alternate Company Security Officer (ACSO) whenever there is a change of personnel who are authorized to access this area.

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

2.2.4.1 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.

2.2.4.2 The foreign contractor must follow all conditions set out in the "IT Security Requirements Document for Contract W8472-105270" and the "Air Gap Computer Document for Contract W8472-105270".

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

2.2.4.4 If unable to adhere to all security requirements, the foreign contractor is required to provide “proposed mitigation measures against specific requirements” which will be reviewed by the DND PO and then discussed with the foreign contractor to determine safeguards acceptable to DND.

2.2.5 Mobile Computing/Teleworking. Mobile computing/teleworking (MC-TW) for contractor employees working from home which involves the IS or Proprietary Information is not authorized for this contract.

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 Secret (Level II) Security Clearance which must be granted and be tracked by PSPC/CSP;

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 W8482-206387 IS, or the zone where the Proprietary Information is being stored / processed / created unless they possess a valid valid Secret (Level II) Security Clearance and are escorted by an authorized contractor employee. An audit log must be maintained of all visitors, foreign nationals or unauthorized personnel accessing the security zone.

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 W8482-206387 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 W8482-206387 IS. 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 security zone and the IS;

2.4.1.3 acceptable use of the IS;

2.4.1.4 incident management procedures;

2.4.1.5 any other subject identified in this document and

2.4.1.6 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 W8482-206387 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 valid Secret (Level II) Security Clearance

2.4.4 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).

2.5.3 Exchange of Proprietary Information. When exchanging Proprietary Information between DND and all levels of contractors/sub-contractors via hard copy and/or removable IT media, all hard copy documents and removable IT media must be handled and transported/transmitted in accordance with GC guidelines as depicted 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 encryption technology approved 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 CCCS publication "*IT Media Sanitization (ITSP.40.006)*".

2.5.6 Controlled Goods. For this contract, the contractor will require access to Confidential and NATO Confidential and Controlled Goods information or equipment.

2.5.6.1 All GC Controlled Goods data (hard and soft copy) must be marked in accordance with DND Defence Administrative Orders and Directives (DAOD) 3003-1. The contractor must abide by all GC Controlled Goods regulations including Controlled Technology Access and Transfer (CTAT) and International Traffic in Arms Regulations (ITAR), where applicable. Additional information can be obtained from the *Controlled Goods Regulations (SOR/2001-32)* (https://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-32/), the DND CTAT office through the DND PO, or the PSPC Controlled Goods Program by email to dmc-cgd@tpsgc-pwgsc.gc.ca.

2.5.6.2 If any Controlled Goods regulations differ from the Information Technology Security Requirements in this document, the most stringent regulation/requirement is to be applied.

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

On a frequency and schedule to be determined by the DND IT Security Authority, DND retains the right to conduct inspections of every contractor's 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 Type of System. The IS must be configured as standalone system.

3.2.2 Type of Equipment. The equipment used to store / process / create the Proprietary Information must consist of Commercial Off The Shelf (COTS) if within a certified MSEC zone otherwise TEMPEST equipment must be used; and must be labelled commensurate with the highest sensitivity level of Proprietary Information to be processed on the equipment.

3.2.3 IS Hard Drives. Processing equipment must be configured with removable hard drives. Examples of processing equipment for this IS include workstations (PCs, laptops, tablets), servers, IT storage devices (network-attached storage (NAS), storage area network (SAN)), printers, scanners, etc.

3.2.4 Operating System. The IS must operate on a supported Operating System (OS); i.e. the vendor of the 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 configured to disable unnecessary processes, services, and ports. The IS SOP must provide details on the OS configuration and identify the frequency and the method used to update the OS security patches.

3.2.5 Anti-virus/Anti-malware Software. A supported anti-virus/anti-malware application must be installed and operating on all workstations and servers (as applicable). Anti-virus/anti-malware definition files must be updated regularly and kept current. The IS SOP must provide details on the configuration of the anti-virus/anti-malware application as well as identify the frequency and the method used to update the anti-virus/anti-malware definition files. Configuration of the anti-virus/anti-malware application must:

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

3.2.5.2 automatically scan all W8482-206387 IS workstations/servers at power-on or on a set interval, at least weekly; and

3.2.5.3 scan every new file introduced to the IS workstations/servers for malicious code.

3.2.6 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.

3.2.7 Logging and Auditing. OS logging must be active and the log files must be reviewed by the W8482-206387 IS system administrator(s) at least monthly. The 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 W8482-206387 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 security zone or the temporary security zone where the IS is located is strictly prohibited except in the case of approved medical devices; the CSO must be advised of all Bluetooth medical devices that are used in the proximity of the W8482-206387 IS.

3.3.4 Wireless or Wi-Fi. The use of wireless or Wi-Fi capabilities on the IS is strictly prohibited.

3.3.5 Cloud Technology. The use of a public or third party "cloud" to store / process / create Proprietary Information is strictly prohibited

3.3.6 Topology Diagram. A topology diagram of the W8482-206387 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.

3.3.7 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 access (e.g. user, power user, 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. !, $, #, %);

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 must:

3.4.3.2.1 be changed at first login;

3.4.3.2.2 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 W8482-206387 IS;

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

3.4.3.2.5 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 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.

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 Air Gap Computer. If the IS is required to interact with untrusted sources (e.g. the internet, another network, removable IT media from another source, etc.) the contractor will be required to provide a standalone Air Gap computer. Data transfer security requirements and related instructions for the Air Gap computer will be provided by the DND PO in a separate technical document; a template for this is available from DIM Secur upon request.

3.5.6 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:

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

3.5.6.2 the IT media's unique identifier;

3.5.6.3 the date and time it was removed;

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

3.5.6.5 the date and time it was returned; and

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

3.6 Personal IT Devices (PITDs)

3.6.1 The contractor must ensure that all Personal IT Devices (e.g. cell phones, smart watches, fit bits, etc.) are kept outside the security zone where the W8482-206387 IS is located.

3.7 Document Printing and/or Reproduction

3.7.1 Printing/Reproduction Authorization. The contractor is:

3.7.1.1 authorized to print and/or reproduce any Proprietary Information within the contractor’s premises using local printing device attached to the IS via tempest cable or fiber optic cable; and

3.7.1.2 not 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 and authorized by PSPC/CSP and the DND PO.

3.7.2 Printing/Reproduction Device Hard Drives. Devices used to reproduce Proprietary Information (e.g. printers, plotters, scanners, photocopiers, MFDs/MFPs, etc.) must be equipped with removable hard drives. If a device does not support removable hard drives a different device, with no hard drive or with a removable hard drive, must be used.

3.7.3 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.

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

3.7.5 Reproduction of Particularly Sensitive Information. For any particularly 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.

3.8 Recovery

3.8.1 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. another building). 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.

3.8.2 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.

3.8.3 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.

3.9 Disposal

3.9.1 Authorization for Disposal. The disposal of all IT media used on 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.

3.9.2 On-Site Disposal. On-site disposal at the contractor's facility of any IT media used to store / process / create Proprietary Information is strictly prohibited.

3.9.3 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 make these IT disposal documents available to PSPC/CSP and the DND PO upon request.

3.9.4 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. Due to the use of control goods by the contractor, the assets with control goods must be demilitarised in coordination with the DND PO.

3.9.5 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.):

3.9.5.1 Any device used to print PC or Classified Proprietary Information on this contract:

3.9.5.1.1 must print at least 50 copies of a page completely filled with unclassified text; this is in order to remove any possible data remaining on the drums, belts or other internal components of the device; and

3.9.5.1.2 must dispose of all toner cartridges by the same method used for disposal of IT media that has failed, is being life cycled, or is no longer

required. This disposal is to prevent security incidents from toner cartridges which contain built-in drums and could retain images of printed documents.

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

3.9.5.3 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.

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

ANNEX C

Appendix 2

Department of National Defence (DND)

Air Gap Computer Document

for

Contract W8482-206387

RELEASE HISTORY

VERSION	AMENDMENT DATE	AMENDMENT DETAILS	AMENDED BY
1.0		Initial draft	
1.1	2021-03-25	Final Submission	Capt Martineau, DIM Secur

TABLE OF CONTENTS

1. INTRODUCTION

1.1 This document outlines the Information Technology (IT) security requirements for Department of National Defence (DND) Contract W8482-206387 for the transfer of electronic information between the Information System (IS) - identified herein for this document only as the W8482-206387 IS - used to store / process / create this contract's Proprietary Information up to and including the level of CONFIDENTIAL or NATO CONFIDENTIAL. The scope of this "Air Gap Computer Document for Contract W8482-206387" is to state the minimum IT security requirements necessary to transfer electronic information to and from the IS.

1.2 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).

1.3 As this contract may require data inputs from untrusted sources, there is a need for an additional level of IT security to mitigate the possibility of infection or malware originating from untrusted sources. These extra steps are intended to protect not only the W8482-206387 IS but also any other system exchanging information with the IS. The transfer of all Proprietary Information into the IS will be required to transition through an Air Gap Computer.

1.4 The application of the IT security safeguards listed in this document are based on the mandatory requirement that the physical premises have been inspected, assessed and authorized to store / process / create information up to and including CONFIDENTIAL or NATO CONFIDENTIAL. Validation must be provided by PSPC/CSP.

2. MANDATORY PREREQUISITES

2.1 Description

2.1.1 A standalone workstation (i.e. PC or laptop) equipped with a removable hard drive as well as two approved and supported anti-virus/anti-malware applications must be used for all electronic data transfers into the IS. The transfer of electronic data into this IS is allowed only from a system of equivalent sensitivity level or lower.

2.1.2 The transfer of electronic data from the W8482-206387 IS must first be authorized in writing by the DND Project Officer (PO).

2.2 Terminology

2.2.1 The following terminology will be used in this document.

Source File	The data to be transferred to the Target System; the Source File must not have a higher sensitivity level than the Target System.
Source System	The IS that the Source File came from.
Target System	The IS that the Source File will be uploaded to. The Target System is the W8482-206387 IS.
Source Transfer Media	The removable electronic media (e.g. CDs/DVDs, USB sticks, SD cards, external hard drives, etc.) containing the Source File from the Source System. For the W8482-206387 IS the type(s) of Source Transfer Media will be DVD only.
Target Transfer Media	The removable electronic media to be used to move the Source File from the W8482-206387 Air Gap Computer to the Target System. For the W8482-206387 IS the type(s) of Target Transfer Media will be DVD only.

2.3 Hardware

2.3.1 This Air Gap Computer must be located in the same physical security zone as the Contract W8482-206387 IS and use the same type of equipment (e.g. COTS or TEMPEST) as stated in section "Type of Equipment" of the "IT Security Requirements Document for Contract W8482-206387".

2.3.2 For the entire length of the contract, this Air Gap Computer must be used only for this purpose.

2.3.3 This Air Gap Computer must be owned by the contractor and be installed, configured, and operational before being inspected by PSPC/CSP.

2.3.4 This Air Gap Computer must consist, preferably, of a stand-alone PC with only a monitor, keyboard and mouse or, alternately, a laptop. No other peripheral equipment (e.g. printer, scanner, etc.) can be attached to the Air Gap Computer.

2.3.5 If using a PC, the Air Gap Computer must be equipped with a removable hard drive.

2.3.6 This Air Gap Computer must be installed and operating in the same security zone zone where the W8482-206387 IS is installed.

2.3.7 Labelling. This Air Gap Computer and removable hard drive (if applicable) must be affixed with a label identifying the highest sensitivity level of the contract's Proprietary Information which is being transferred using this equipment.

2.3.8 Labelling of Transfer Media. The Transfer Media to be used on this Air Gap Computer must be marked with the following information:

2.3.8.1 the highest sensitivity level of the data it contains,

2.3.8.2 the government department (in this case DND),

2.3.8.3 the contract number (in this case W8482-206387),

2.3.8.4 the IT media's unique identifier, as discussed in para 3.5.3.2 of the "IT Security Requirements Document for Contract W8482-206387", and

2.3.8.5 the transfer media category (either "Source Transfer Media" or "Target Transfer Media").

2.3.9 If this information cannot be written directly on the media or if a large label (approximately 4" by 6") cannot be affixed directly on the media, the label must be attached to the IT media by other means (e.g. string, etc.).

2.3.10 The "Source Transfer Media" and the "Target Transfer Media" should be labelled with different colours (e.g. black for one, red for the other) to easily differentiate between them.

Figure 1: example labels

2.4 IT System Configuration

2.4.1 This Air Gap Computer must operate on a supported Operating System (OS) and must follow all items specified in the paragraph "Operating System" of the "IT Security Requirements Document for Contract W8482-206387". As well as disabling unnecessary processes, services, and ports, all unnecessary computer components (e.g. network card, microphone, speakers, etc.) must also be disabled.

2.4.2 Two different anti-virus/anti-malware applications must be installed on this contract's Air Gap Computer and these applications must be supported. This contract's Air Gap Computer must follow all items specified in the paragraph "Anti-virus/Anti-malware Software" of the "IT Security Requirements Document for Contract W8482-206387".

2.4.3 Any other applications installed on this contract's Air Gap Computer shall be deleted/uninstalled, and no other applications can be installed on this computer.

2.4.4 OS logging must be active on this contact's Air Gap Computer, and all items specified in the paragraph "Logging and Auditing" of the "IT Security Requirements Document for Contract W8482-206387" must be followed.

2.4.5 All accounts on this contact's Air Gap Computer must follow the applicable sections of the paragraph "Authorization and Access Control" of the "IT Security Requirements Document for Contract W8482-206387". No shared or generic accounts are authorized.

2.4.6 The following paragraphs of the "IT Security Requirements Document for Contract W8482-206387" are applicable to this Air Gap Computer and must be followed:

- "Unattended Removable Media";
- "IT Media";
- "Personal IT Devices (PITDs)"; and
- "Disposal".

2.5 Air Gap Computer and SOP

2.5.1 The W8482-206387 IS SOP must include the procedures and details mentioned in this "Air Gap Computer Document for Contract W8482-206387" for all applicable aspects of this Air Gap Computer.

3. DATA TRANSFER PROCEDURES

3.1 The following process must be used to transfer electronic data from any untrusted source(s) to the IS.

3.2 These Data Transfer Procedures must be posted near the W8482-206387 Air Gap Computer.

DATA TRANSFER PROCEDURES

1. Power on the W8482-206387 Air Gap Computer and logon.
2. Ensure that the definition files for both anti-virus/anti-malware applications are current. If not current, update the necessary definition files before proceeding.
3. Copy the Source File(s) from the Source System to the Source Transfer Media. If the Source File(s) is/are already on removable electronic media (e.g. removable media received from a vendor, etc.), then this can be used as the Source Transfer Media.
4. Label the Source Transfer Media and connect it to the Air Gap Computer.
5. Scan the Source Transfer Media and all Source File(s) using both anti-virus/anti-malware applications.
   a. If any viruses/malware are detected, STOP the procedure. Clean/delete the file(s) as directed by the anti-virus/anti-malware applications and inform the Company Security Officer (CSO) or the Alternate Company Security Officer (ACSO).
   b. If no viruses/malware are detected, proceed to the next step.
6. Copy the Source File(s) from the Source Transfer Media onto the Air Gap Computer.
7. Remove the Source Transfer Media from the Air Gap Computer.
8. Label the Target Transfer Media and connect it to the Air Gap Computer.
9. Copy the scanned Source File(s) from the Air Gap Computer to the Target Transfer Media.
10. Remove the Target Transfer Media from the Air Gap Computer.
11. Connect the Target Transfer Media to the Target System.
12. Copy the scanned Source File(s) from the Target Transfer Media to the Target System.
13. Ensure that the scanned Source File(s) copied to the Target System can be opened and are not corrupted.
14. If the Source File(s) on the Target System is/are satisfactory:
    a. delete the Source File(s) from the Target Transfer Media;
    b. remove the Target Transfer Media from the Target System; and
    c. delete the Source File(s) from the Air Gap Computer.
15. Log off and shut down the Air Gap Computer.

ALL OTHER TERMS AND CONDITIONS OF THE SOLICITATION (RFP) REMAIN UNCHANGED