Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8472-135462/002/qf
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
DEPARTMENT OF NATIONAL DEFENCE	ADM(MAT) DGMEPM/DNCS
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

Acquisition and In-Service Support for the Underwater Warfare Suite Upgrade of the Underwater Weapons Warfare Suite for the Halifax-class frigates and trainer facilities. Delivery to include: equipment systems, installation Technical Data Package, documentation, software, test forms, trials, training documents and initial cadre training, In-Service Support activities to include: Service delivery of engineering support, maintenance support, material support, Life cycle material management, configuration management and repair and overhaul activities.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non ☐	Yes / Oui ☑
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	No / Non ☐	Yes / Oui ☑

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non ☐	Yes / Oui ☑
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	No / Non ☑	Yes / Oui ☐
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	No / Non ☑	Yes / Oui ☐

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

Canada ☑	NATO / OTAN ☑	Foreign / Étranger ☑
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions Aucune restriction relative à la diffusion ☑	All NATO countries Tous les pays de l'OTAN ☑	No release restrictions Aucune restriction relative à la diffusion ☐
Not releasable À ne pas diffuser ☑		
Restricted to: / Limité à : ☑	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☑
Specify country(ies): / Préciser le(s) pays : Canadian Citizens and Permanent Residents and citizens of NATO, Australia and New Zealand. Les citoyens canadiens et résidents permanents et de NATO, Australie et Nouvelle-Zélande	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays : Respective citizens of Canada, United States, Australia, United Kingdom and New Zealand - Citoyens respectifs des États-Unis, Australie, Royaume-Uni, Nouvelle-Zélande et Canada
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
W8472-135462/002/qf
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?

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
W8472-135462/002/qf
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 / TRÈS 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
W8472-135462/002/qf
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
Len Terpstra	DNCS 4-7	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
819-939-3310	819-939-3622	Len.Terpstra@forces.gc.ca	31 Oct 2016

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Dawn Murray - DDSO - Industrial Security SRCL Team Lead Tel: 613-996-0274 E-mail: dawn.murray@forces.gc.ca		Dawn Murray

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
			8 November 2016

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
LAURA SAMPLE	Procurement Authority	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
819-939-3064	Ø	laurasample@forces.gc.ca	16 Feb 17

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

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

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
			January 23, 2017

Sherry Campbell
Contract Security Officer, Contract Security Division
Sherry.Campbell@tpsgc-pwgsc.gc.ca
Tel/Tél - 613-948-1646 / Fax/Téléc - 613-948-1712

Security Requirement Checklist (SRCL) Supplemental Security Guide

Guide de sécurité supplémentaire de la liste de vérification des exigences de sécurité (LVERS)

Part A - Multiple Release Restrictions: Security Guide SRCL

To be completed in addition to SRCL question 7.b) when release restrictions are therein identified. Indicate to which levels of information release restrictions apply. Make note in the chart if a level of information bears multiple restrictions (e.g. a portion of the SECRET information bears the caveat Canadian Eyes Only while the remainder of the SECRET information has no release restrictions.)

Partie A - Restrictions de libération multiple: Guide de sécurité SRCL

À compléter en plus de la question 7.b) de la LVES, lorsque des restrictions de mainlevée sont identifiées. Indiquez à quels niveaux de restrictions de diffusion de l'information s'appliquent. Notez dans le tableau si un niveau d'information porte de multiples restrictions (par exemple, une partie des informations SECRET porte la mise en garde Canadian Eyes Only tandis que le reste de l'information SECRET n'a pas de restrictions de publication).

Canadian Information

Canada information not specifically annotated as CEO and not otherwise caveat annotated, is releasable to citizens of the following countries provided individuals also hold respective clearances: Canada (including Canadian Permanent Residents), a NATO country, AUS or NZ.

Canada information annotated as CEO is only releasable to Canadian citizens (does not include Canadian Permanent Residents) provided individuals also hold respective clearances.

Information Canadienne

Canada, y compris les résidents permanents canadiens, un pays de l'OTAN, l'AUS ou la Nouvelle-Zélande.

Les renseignements du Canada annotés en tant que PDG ne peuvent être divulgués qu'aux citoyens canadiens (ne comprend pas les résidents permanents du Canada) à condition que les personnes détiennent également les autorisations nécessaires.

Citizenship Restriction	PROTECTED			CLASSIFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions	X	X					
Not Releasable				X	X		
Restricted to: NATO Countries, AUZ, NZ				X	X		
Permanent Residents Included*				X	X		

NATO Information

NATO information not otherwise caveat annotated is releasable to citizens of NATO countries (includes Canadian Permanent Residents for Canada) provided individuals also hold respective clearances

Informations de l'OTAN

L'information de l'OTAN autrement annulée ne peut être communiquée aux citoyens des pays de l'OTAN (y compris les résidents permanents canadiens pour le Canada)

Citizenship Restriction	NATO UNCLASSIFIED	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET
All NATO Countries	X	X	X	X	
Restricted to:NATO Countries					
Permanent Residents Included*					

Foreign Information

Foreign information specifically caveat annotated is only releasable to citizens of respective foreign countries (does not include Canadian Permanent Residents for Canada) provided individuals also hold respective clearances

Information étrangère

L'information étrangère spécifiquement réservée annotée n'est libérable que pour les ressortissants de pays étrangers respectifs (ne comprend pas les résidents permanents canadiens pour le Canada) à condition que les individus détiennent aussi les autorisations respectives

Citizenship Restriction	PROTECTED			CLASSIFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions							

Restricted to : Canada, United States, Australia, United Kingdom and New Zealand				X	X		
Permanent Residents Included*							
COMSEC Information							
Citizenship Restriction	PROTECTED			CLASSIFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
Not Releasable							
Restricted to:							
DND ONLY Embedded Contractor (Access to Controlled Goods) MDN SEULEMENT Embarqué Entrepreneur (Accès aux marchandises contrôlées)							
Restriction	Yes				NO		
SECRET clearance with CEO applies							

***When release restrictions are indicated, specify if permanent residents are allowed to be included.**
*** Lorsque des restrictions de libération sont indiquées, précisez si les résidents permanents peuvent être inclus.**

Part B - Multiple Levels of Personnel Screening: Security Classification Guide SRCL

To be completed in addition to SRCL question 10.a) when multiple levels of personnel screening are therein identified. Indicate which personnel screening levels are required for which portions of the work/access involved in the contract.

Partie B - Niveaux multiples de contrôle du personnel: Guide de classification de la sécurité SRCL
À compléter en plus de la question 10.a) de la LVERS, lorsque des niveaux multiples de dépistage du personnel y sont identifiés. Indiquer quels niveaux de dépistage du personnel sont requis pour quelles parties du travail / accès impliqués dans le contrat.

Level of Personnel Clearance (e.g. Reliability, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
Reliability Status	Limited program execution stages and tasks (if any) specifically deemed/approved as unclassified or not sensitive in nature. Étapes limitées d'exécution du programme et tâches (le cas échéant) spécifiquement jugées / approuvées	Limited areas of Manufacturer production facilities, limited program execution stages/tasks and/or program information (if any) specifically deemed/approved as unclassified or not sensitive in nature. Specifically approved (limited) unclassified/non-sensitive visits to DND facilities	n/a

	non classifiées ou non sensibles	Zones limitées des installations de production du fabricant, étapes limitées d'exécution du programme / tâches et / ou informations sur le programme (le cas échéant) spécifiquement jugées / approuvées comme non classifiées ou non sensibles. Visites non classifiées / non-sensibles spécifiquement approuvées (limitées) aux installations du MDN	
Confidential	Limited program execution stages and tasks (if any) specifically deemed/approved as not greater than Confidential in nature. Étapes limitées d'exécution du programme et tâches (le cas échéant) spécifiquement jugées / approuvées comme ne dépassant pas le caractère confidentiel.	Limited areas of Manufacturer production facilities, limited program execution stages/tasks and/or program information (if any) specifically deemed/approved as not greater than Confidential. Les zones limitées des installations de production du fabricant, les étapes limitées d'exécution du programme ou les tâches et / ou les informations sur le programme (le cas échéant) sont spécifiquement jugées / approuvées comme étant non confidentielles.	Canada (including Canadian Permanent Residents), NATO countries, AUS or NZ. Canada (y compris les résidents permanents canadiens), les pays de l'OTAN, l'AUS ou la Nouvelle-Zélande.
Secret	All program execution stages and tasks unless otherwise specifically approved. Tous les stades	Required for access to DND Dockyards, HMC Ships and DND shore sites. All program information unless specifically otherwise deemed/approved.	Canada (including Canadian Permanent Residents), NATO countries, AUS or NZ. Canada (y compris les résidents permanents

	d'exécution du programme et les tâches à moins d'être expressément approuvé autrement.	Obligatoire pour l'accès aux chantiers navals du MDN, aux navires de la NCSM et aux sites côtiers du MDN. Tous les renseignements sur le programme, à moins qu'il ne soit autrement spécifié / approuvé.	canadiens), les pays de l'OTAN, l'AUS ou la Nouvelle-Zélande.
NATO Confidential NATO Secret	Limited program execution stages and tasks specifically deemed as related to NATO Confidential or NATO Secret material or information. Étapes limitées d'exécution du programme et tâches spécifiquement considérées comme liées aux informations confidentielles de l'OTAN ou à l'OTAN.	Program execution stages (Manufacturer production at own facilities and/or at DND facilities/sites) related to not greater than (respectivedly) NATO Confidential or NATO Secret Documents and information. Étapes de l'exécution du programme (production du fabricant dans les installations propres et / ou dans les installations / sites du MDN) relatives à des documents et renseignements secrets de l'OTAN (respectivedement) ou non confidentiels de l'OTAN.	NATO Countries (including Canadian Permanent Residents for Canada). Pays de l'OTAN (y compris les résidents permanents canadiens pour le Canada).
NATO Restricted	Limited program execution stages and tasks specifically deemed as related to NATO Restricted material or information. Étapes limitées d'exécution du programme et tâches spécifiquement jugées liées à l'OTAN Matériel ou	Program execution stages (Manufacturer production at own facilities and/or at DND facilities/sites) related to not greater than NATO Restricted Documents and information. Étapes d'exécution du programme (production du fabricant dans les installations propres et / ou dans les installations / sites du MDN) concernant des documents et des	NATO Countries (including Canadian Permanent Residents for Canada). Pays de l'OTAN (y compris les résidents permanents canadiens pour le Canada).

	information restreint.	renseignements non restreints de l'OTAN.	
SECRET CEO	Specifically identified stages or portions of program execution related to: integration, deficiency reporting, vulnerability assessments, documentation of system capabilities and limitations, documentation of system performance against live targets, test and trial results, sensor and system testing, progress status reporting for compliances, and system data and performance results when operating with CEO dataBases loaded. Étapes et parties de l'exécution du programme spécifiquement identifiées concernant: l'intégration, la déclaration de déficiences, les évaluations de vulnérabilité, la documentation des capacités et des limites du système, la documentation de la performance du système par rapport aux cibles vivantes, les résultats des essais et des essais, Et les données	Specifically identified information related to program integration, deficiency reporting, vulnerability assessments, documentation of system capabilities, documentation of performance, test and trial results, sensor and system testing, progress status reporting for compliances. All information related to operational databases and operational detections. Des renseignements précis sur l'intégration des programmes, les rapports sur les carences, les évaluations de la vulnérabilité, la documentation des capacités du système, la documentation des performances, les résultats des essais et des essais, les tests des capteurs et des systèmes, Toutes les informations relatives aux bases de données opérationnelles et aux détections opérationnelles.	Canadian Citizens Only (does not include permanent residents) Citoyens canadiens seulement (ne comprend pas les résidents permanents)

	système et les résultats de performance lorsqu'ils fonctionnent avec des bases de données PDG chargées.		

Part C – Safeguards / Information Technology (IT) Media – 11d = yes
Partie C - Mesures de sauvegarde / Technologie de l'information (TI) - 11d = oui
Yes: Classified and sensitive Documents and details related to military Equipment and Operating Software will be produced by this contract iaw the SOW, PWS and CDRLs. The design, development, test, trails and acceptance program/processes under this contract will produce some information and insight related to system and capabilities, limitations, deficiencies, performance and vulnerabilities that will be specifically deemed as Secret-CEO. Oui: Classifiés et sensibles Les documents et les détails relatifs à l'équipement militaire et au logiciel d'exploitation seront produits par le présent contrat, à savoir les normes SOW, PWS et CDRL. La conception, le développement, les essais, les pistes et le programme d'acceptation dans le cadre du présent contrat produiront des renseignements et des renseignements sur le système et les capacités, les limitations, les lacunes, les performances et les vulnérabilités qui seront spécifiquement considérés comme secrets.

OTHER SECURITY INTRUCTIONS

AUTRES INSTRUCTIONS DE SÉCURITÉ

• Canadian Information identified as CEO provided or produced under this contract is to only be released to Canadian citizens. Information provided or produced under this contract can only be viewed by contractor personnel holding the requisite clearance. NATO or specific Foreign only identified information is restricted to citizens of a NATO Member country (including Canadian permanent residents for Canada) or respective foreign citizens, cleared to the requisite level. •CLASSIFIED information and assets exchanged or generated in connection with this contract will be used, transmitted and safeguarded iaw the government Security Policy and procedures for which, Contractor Personnel working on their own sites are contained in the Industrial Security Manual. Contractor Personnel working on DND sites shall abide by the National defence Security Instructions. •DND Security Supervisors are responsible to brief Contractor employees on these policies and any other security instructions/policies as required. • Foreign Contractors will abide by their Governments' national security regulations and/or bilateral agreements and MOU's. • Prior to having access to NATO information and Assets, Contractor Personnel must hold a valid NATO Security Clearance and are required to sign a copy of the NATO procedures for safeguarding such

information and assets iaw the provisions of NATO C-M(2002)49.

• Prior to allowing any access to CLASSIFIED information, assets or secure premises, confirmation of Contractor personnel's security clearances must be forwarded on a Visit Clearance Request through the Canadian and International Industrial Security Division (CIISD) of Public Services and Procurement Canada (PSPC). For approval and bear the name of this contract/program/project/contract number and the Project Officer.

• Contractor personnel requiring access to the National Defence Wide Area Network (DWAN), must be registered and cleared to the requisite level with the CIISD – Controlled Goods Program (CGP), prior to being given a network account.

• Classified documents and/or assets which require transmittal between National defence and the Contractor(s), must be co-ordinated through approved official channels. Sensitive information transactions within Canada may be forwarded directly to the Company Security Officer or designated alternate. A copy of the document transmittal form must be provided to the Document Control Section of the CIISD at the following address:

Public Services and Procurement Canada
Canadian and International Industrial Security Division
Document Control Section2745 Iris St.
Ottawa, Ontario, Canada K1A 0S5

• Foreign CLASSIFIED information and/or any information that is to be sent to foreign company must be shipped through Government-to-Government channels via CIISD.

•At no time will be contractor be allowed Information Technology Connections to DND without the express consent of DND NDHQ Security authorities. The internet shall not be used in a manner that results in a security infraction under DND or Government security policies.

• All CLASSIFIED documents, reports, systems and/or assets developed and extensions thereto under any tasking related to this contract shall not be reproduced or divulged/disseminated to a third party without the prior written permission of DND. Improper or unauthorized disclosure of this information may constitute an offence under the Security of Information Act.

• Subcontracts containing security requirements are prohibited without the prior written authorization from CIISD/PSPC.

• During the Development and initial operational phases and trials of the UWSU Equipment Group (EG), either aboard HMCS Frigates or in shore based facilities, the UWSU recorded data archives and information electronically produced are not to be annotated when recorded. Development and operations teams working on the UWSU EG are not to conduct any actions during the acquisition and trailing phases of this contract that may result in the production of 'Canadian Eyes Only' (CEO) Classified records and the Teams are to be advised to avoid this. Recorded data sets or circuit cards containing Non-volatile memory have been annotated or that are identified as having been annotated as CEO Classified records are not to be released back to the Contractor. The potential production of CEO records is to be monitored on a per platform basis.

• Once Operational Databases for shipboard or Trainer use are generated and CEO records are annotated, the processing systems and operational Data Sets will become SECRET CEO on a permanent and ongoing basis. Performance, vulnerability and deficiency results and assessments from the design, development and trials/test/acceptance program may also be identified as CEO.

• L'information canadienne identifiée comme chef de la direction fournie ou produite dans le cadre du présent contrat ne doit être divulguée qu'aux citoyens canadiens. Les informations fournies ou produites en vertu du présent contrat ne peuvent être consultées que par le personnel de l'entrepreneur qui détient l'autorisation requise. L'OTAN ou les renseignements spécifiques étrangers

uniquement sont réservés aux citoyens d'un pays membre de l'OTAN (y compris les résidents permanents canadiens pour le Canada) ou à des ressortissants étrangers respectifs, autorisés au niveau requis.

• Les informations et les biens CLASSIFIÉS échangés ou générés dans le cadre du présent contrat seront utilisés, transmis et protégés par la Politique de sécurité du gouvernement et les procédures pour lesquelles le Personnel contractuel travaillant sur ses propres sites est contenu dans le Manuel de sécurité industrielle. Le personnel de l'entrepreneur travaillant sur les sites du MDN doit se conformer aux Instructions de sécurité de la Défense nationale.

• Les superviseurs de la sécurité du MDN sont chargés d'informer les employés de l'entrepreneur de ces politiques et de toutes autres instructions / politiques de sécurité, au besoin.

• Les entrepreneurs étrangers se conformeront aux règlements de sécurité nationale de leurs gouvernements et / ou aux accords bilatéraux et aux PE.

• Avant d'avoir accès aux informations et aux biens de l'OTAN, le personnel de l'entrepreneur doit détenir une attestation de sécurité valide de l'OTAN et doit signer une copie des procédures de l'OTAN pour la sauvegarde de ces informations et biens conformément aux dispositions de l'OTAN C-M (2002) 49.

• Avant de permettre l'accès aux renseignements, biens ou locaux sécurisés CLASSIFIÉS, la confirmation des autorisations de sécurité du personnel de l'entrepreneur doit être transmise par l'intermédiaire de la Division de la sécurité industrielle canadienne et internationale (DSICI) des Services publics et Approvisionnement Canada (PSPC). Pour approbation et porter le nom de ce contrat / programme / projet / numéro de contrat et l'agent de projet.

• Le personnel de l'entrepreneur qui a besoin d'avoir accès au réseau de zone étendue de la Défense nationale doit être enregistré et dédouané au niveau requis avec le Programme de marchandises contrôlées de la CIISD avant d'obtenir un compte de réseau.

• Les documents classifiés et / ou les biens qui nécessitent une transmission entre la Défense nationale et le (s) contractant (s) doivent être coordonnés par des voies officielles approuvées. Les opérations d'information confidentielles au Canada peuvent être transmises directement à l'agent de sécurité de l'entreprise ou à son remplaçant désigné. Une copie du formulaire de transmission du document doit être fournie à la Section de contrôle des documents de la DSICI à l'adresse suivante:
Services publics et approvisionnement Canada
Division de la sécurité industrielle canadienne et internationale
Section de contrôle des documents2745 Iris St.
Ottawa, Ontario, Canada K1A 0S5

• Les renseignements CLASSIFIÉS à l'étranger et / ou toute information qui doit être envoyée à une société étrangère doivent être expédiés par l'entremise de canaux de gouvernement à gouvernement via la DSICI.

• À aucun moment, l'entrepreneur ne sera autorisé. Connexions de la technologie de l'information au MDN sans le consentement exprès du MDN. L'Internet ne doit pas être utilisé d'une manière qui entraîne une infraction à la sécurité en vertu des politiques de sécurité du MDN ou du gouvernement.

• Tous les documents, rapports, systèmes et / ou actifs CLASSIFIÉS élaborés et extensions de ceux-ci dans le cadre de toute tâche reliée au présent contrat ne doivent pas être reproduits, divulgués ou diffusés à un tiers sans l'autorisation écrite préalable du MDN. La divulgation inappropriée ou non autorisée de ces renseignements peut constituer une infraction à la Loi sur la protection de l'information.

• Les contrats de sous-traitance contenant des exigences de sécurité sont interdits sans l'autorisation écrite préalable de CIISD / PSPC.

• Pendant les phases de développement et d'exploitation initiale et les essais du Groupe d'équipement UWSU (EG), soit à bord du NCSM Frigates, soit dans des installations à terre, les archives de données enregistrées UWSU et les informations produites électroniquement ne doivent pas être annotées

lorsqu'elles sont enregistrées. Les équipes de développement et d'exploitation qui travaillent sur l'UWSU EG ne doivent pas mener d'actions durant les phases d'acquisition et de fin de ce contrat qui peuvent aboutir à la production de disques classés «Canadian Eyes Only» et les équipes doivent être avisées d'éviter ce. Les ensembles de données enregistrés ou les cartes à circuit imprimé contenant des mémoires non volatiles ont été annotés ou identifiés comme ayant été annotés, car les dossiers classés par le CEO ne doivent pas être remis à l'Entrepreneur. La production potentielle des dossiers des PDG doit être surveillée par plate-forme.

• Une fois que les bases de données opérationnelles pour l'utilisation à bord ou pour le formateur sont générées et que les dossiers des PDG sont annotés, les systèmes de traitement et les ensembles de données opérationnels deviendront le CEO SECRET de façon permanente et continue. Les résultats et les évaluations du rendement, de la vulnérabilité et de la carence ainsi que les évaluations du programme de conception, de développement et d'essais / d'essai / d'acceptation peuvent également être identifiés comme PDG.

IT Security Requirements

For

Contracts W8472-135462/001/qf and W8472-135462/002/qf

Between

Department of National Defence (DND)

And

{Contractor Name}

1. INTRODUCTION

This document outlines the Information Technology (IT) Security requirements for the Department's contracts W8472-135462/001/qf and W8472-135462/002/qf with {Contractor Name} for the processing of sensitive data up to and including the level of Secret CEO, NATO Secret and Foreign Secret. In absence of a formal Threat-Risk Assessment (TRA) and due to the IT portion of the Security clearance being contract specific, the intent of this document is to state the minimum IT Security safeguards required in order that the processing of sensitive information be approved by the Department of National Defence's IT Security Coordinator (ITSC).

Security is based upon layers of protection; that is, in order for the requirements of the IT Security (ITSEC) to effectively safeguard the information, they must be preceded and supported by other aspects of security and the associated policies. The physical, personnel and information security safeguards in accordance with the Policy on Government Security (PGS) and ITSEC related Policy, Directive and Standards must exist *prior* to the implementation of ITSEC safeguards.

2. MANDATORY PREREQUISITES

2.1. PWGSC Validation for Physical Security

The application of the ITSEC safeguards listed in this document are based on the *mandatory requirement* that the physical premises have been inspected, assessed and authorized to process and store sensitive data up to and including the level of Secret CEO, NATO Secret and Foreign Secret information by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services (PWGSC). Upon validation, CISD will notify the Department of National Defence (DND) Project Lead, the Director Defence Security Operations (DDSO) Industrial Security Lead and Director Information Management Security (DIM Secur) Operations of the successful completion of this requirement through the Facility Security Clearance (FSC).

2.2. Personnel Security

All personnel who have access to the material being processed must be a respective citizen of CANADA (or permanent resident of Canada for NATO only data), a citizen of a NATO country, or a citizen of the respective Foreign country, and must each hold the valid respective personnel security screening up to the level of Secret, as required, granted in accordance with the national policies of CANADA and have a "*need to know*".

2.3. Information Security

All hard copy documents and other media formats transferred to {Contractor Name} must be handled and transported in accordance with Government of Canada guidelines. All hard copy documents and other media will be marked with the appropriate security designation or classification, packaged appropriately and be transferred with a covering letter, transmittal form or circulation slip marked to indicate the highest level of designation or classification of the attachments as stated in the contracts Security Requirements Check List (SRCL).

3. MINIMUM IT SECURITY REQUIREMENTS

3.1. IT Security Policy Compliance and Monitoring

On a frequency to be determined by the Departmental IT Security Coordinator, DND retains the right to conduct inspections of the {Contractor Name} facility to ensure compliance with Government of Canada standards and policies with respect to prevention, detection, response and recovery requirements in the *Operational Security Standard: Management of Information Technology Security* (MITS).

3.2. Adherence to Government Policies

All information technology operations related to ITSEC incident prevention, detection, response and recovery must adhere to MITS sections 16 to 18.

3.2.1 Prevention

Prevention safeguards protect the confidentiality, integrity, and availability of information and IT assets.

3.2.1.1 Physical Security within the IT Security Environment

The equipment used to process the sensitive information must be either standalone or part of an authorized standalone network designated for the storage and processing of up to and including the level of Secret CEO, NATO Secret and Foreign Secret data related to the contract located in a(n) {Zone Type} Zone as outlined in the Treasury Board of Canada Secretariat (TBS) Operational Security Standard on Physical Security (OSSPS). This standalone network must only be used to process and store data related to contracts with DND and no other customer or party.

3.2.1.2 Cryptography, Network Security and Perimeter Defence

The electronic storage of up to and including the level of Secret CEO, NATO Secret and Foreign Secret information associated with this contract must be within a CISD approved IT environment.

Electronic transmission of Protected A information should be encrypted when supported by a Threat and Risk Assessment. However, Protected B and higher information must be encrypted. For Protected B information and higher, the {Contractor Name} must segregate their respective networks into IT security zones and implement perimeter defence and network security safeguards. CSEC provides the ITSG-38 and ITSG-22 guidelines on this specific subject. As well, the Contractor/Supplier must apply strict control of all access to the protected zone where the information associated with this contract resides. Network perimeter defence safeguards (e.g. firewalls, routers) must be used to mediate all traffic and to protect servers that are accessible from the internet. The {Contractor Name} must use CSEC approved encryption technology to ensure confidentiality, integrity, authentication and non-repudiation.

The "*need to know*" principle must always be applied for sensitive information and transmission must be restricted only to CISD approved recipients.

3.2.1.3 Storage, Disposal and Destruction of IT Media

All material such as CD/DVDs, flash/thumb drives, workstation hard disks, server hard disks, backup tapes and any other devices used to process or store sensitive information must be identified and itemized by designation or classification, releasability caveat, model and serial number for hard disks, and by designation or classification, releasability caveat and a unique identification number for any other media or devices which cannot be identified by model or serial number. These devices or material must be retained and properly stored or disposed of by the DND Project Lead in the event of failure and replacement of the equipment or termination of the final contract. All destruction of devices or material must be authorized in advance by the DND Project Lead.

The DND Project Lead must be provided with the list of equipment and media being used. In addition, only equipment and media that has been identified, itemized and documented may be used to process sensitive information associated with DND contracts.

In the event that equipment requires maintenance, support or replacement, no hardware associated with the processing or storage of sensitive information may be given to an outside vendor.

3.2.1.4 Authorization and Access Control

{Contractor Name} must provide the DND Project Lead with a list of all individuals who have access to the sensitive information being processed for the Department, along with {Contractor Name} current policies and procedures for adding individuals to the environment and the process followed when an individual is removed from the environment.

In following the principle of "least-privilege", the {Contractor Name} must provide only the minimum access required for individuals to perform their duties.

3.2.1.5 Mobile Computing and Teleworking

Due to the fact that the requirements have stipulated a stand-alone network configuration, mobile computing and teleworking need not be expressly addressed; however, it is important to state that the processing of sensitive information associated with DND-related contracts *may only* be performed in the facility which has been authorized by CISD.

3.2.1.6 Emanations Security

{Contractor Name} shall adhere to Government emanations security (EMSEC) policies. This includes, but is not limited to, the consideration for both the use of TEMPEST-certified equipment and the development and implementation of facility-specific wireless communications usage policies.

3.2.1.7 Telecommunications Cabling

Access to cabling used for interconnection of devices used to process/manage/store DND sensitive information is to be controlled and monitored to prevent inadvertent or deliberate connection to any other network or infrastructure.

3.2.1.8 Software Integrity and Security Configuration

{Contractor Name} shall configure the security of their operating systems and application software being used to process DND sensitive information in accordance with Government of Canada requirements. Software patches for all applications and services running on the equipment used to store, manage or process DND sensitive information must be kept up to date and managed through a defined configuration management process.

3.2.1.9 Malicious Code

Due to the isolation of the systems being used to process sensitive information (standalone system or standalone network) these systems are less exposed to malicious code such as viruses, Trojan horses, and network worms; however, without proper procedures for introducing new equipment or information into the environment, they are still vulnerable. Therefore, {Contractor Name} must install, use and regularly update antivirus software and conduct scans on all electronic files from external systems.

3.2.2 Detection

It is important to have the ability to detect security related issues within the operating environment which processes DND sensitive information. Even though the systems are isolated, it is still useful to use sources such as system logs (event viewer), virus protection software and other system tools to monitor systems. Therefore, {Contractor Name} must implement a capability to detect activity such as unauthorized access, unplanned disruption of systems or services or unauthorized changes to system hardware, firmware, or software.

3.2.3 Response and Recovery

3.2.3.1 Incident Response

The PGS requires departments to 'establish mechanisms to respond effectively to IT incidents and exchange incident-related information with designated lead departments in a timely fashion'. Similarly, DND requires {Contractor Name} to have a documented incident response process. Details of the incident response process are to be provided in a document to the DND Project Lead for review and endorsement.

3.2.3.2 Incident Reporting

It is paramount that the DND Project Lead be made aware of all security-related incidents with respect to the facilities and equipment used to process and store DND sensitive information associated with DND contracts.

{Contractor Name} must report any security-related incidents to the DND Project Lead identified below by 1200 hrs the day after a security incident has been detected or reported.

3.2.3.3 Recovery

The ability to recover systems and information is extremely important in any IT environment. DND requires {Contractor Name} to demonstrate the ability to address systems recovery by providing documentation relating to systems and server backup policies (e.g. processes used, tests restores, retention periods and storage of backup media) for the equipment to be used in the processing of DND sensitive information. Details of the safeguards are to be provided in a document to the DND Project Lead for review and endorsement.

Exigences relatives à la sécurité des technologies de l'information (TI)

Pour les contrats

W8472-135462/001/qf and W8472-135462/002/qf

Entre

Ministère de la Défense nationale (MDN)

Et

{Nom de l'entrepreneur}

1. INTRODUCTION

Ce document traite des exigences de sécurité pour les technologies de l'information (TI) dans le cadre des contrats W8472-135462/001/qf and W8472-135462/002/qf conclu entre le Ministère et {Nom de l'entrepreneur} relativement au traitement de données protégés/classifiés Secret et réservé aux canadiens, Secret de l'OTAN, et Secret étranger ou de niveau inférieur. Faute d'une évaluation de la menace et des risques officielle (EMR) et parce que les exigences pour les TI visant l'autorisation de sécurité sont particulières au contrat, ce document vise à présenter les mesures de sécurité minimales nécessaires pour que le traitement de renseignements protégés/classifiés soit approuvé par le coordonnateur de la sécurité des TI du MDN.

La sécurité repose sur diverses protections. En d'autres termes, les exigences de sécurité pour les TI, lorsqu'elles sont respectées, permettent de protéger l'information efficacement seulement si d'autres mesures et politiques de sécurité les sous-tendent. Les mesures de protection concernant les lieux, le personnel et la sécurité de l'information conformes à la Politique sur la sécurité du gouvernement et à la politique, la directive et les normes connexes de sécurité pour les TI doivent avoir été mises en application *avant* la mise en œuvre des sauvegardes de sécurité des TI.

2. EXIGENCES PRÉALABLES OBLIGATOIRES

2.1. Validation de la sécurité des lieux par Services publics et Approvisionnement Canada (SPAC)

L'application des mesures de sécurité des TI énoncées dans ce document est conditionnelle à l'inspection, à l'évaluation, et à l'autorisation *obligatoires* des lieux en vue du traitement et du stockage de renseignements protégés/classifiés jusqu'à et y compris le niveau de Secret et réservé aux canadiens, Secret de l'OTAN, et Secret étranger par la Direction de la sécurité industrielle canadienne (DSIC) du ministère des Services publics et Approvisionnement Canada. Lors de la validation, la DSIC informera le chef de projet du ministère de la Défense nationale (MDN), le chef de la sécurité industrielle du directeur des opérations de sécurité de la Défense, et le directeur – sécurité (gestion de l'information) (Dir Sécur GI) des opérations de la réussite de cette exigence au moyen de l'attestation de sécurité d'installation (ATI).

2.2. Sécurité du personnel

Tous les membres du personnel ayant accès aux données traitées doivent être un citoyen respectif canadien (ou un résident permanent du Canada pour les seules données de l'OTAN), un citoyen d'un pays de l'OTAN, ou un citoyen du pays étranger concerné, et doivent chacun détenir le contrôle de sécurité du personnel valide respectif jusqu'au niveau de Secret, selon le besoin, accordé conformément aux politiques nationales du CANADA ainsi qu'avoir le « besoin de savoir ».

2.3. Sécurité de l'information

Les documents en version papier et sur d'autres supports, transférés à {Nom de l'entrepreneur}, doivent être manipulés et transportés conformément aux directives du gouvernement du Canada. Il faut y indiquer le niveau de désignation ou de classification de sécurité applicable, les emballer de façon appropriée, et les transférer avec une lettre de présentation, une formule d'accompagnement ainsi qu'un bordereau de circulation indiquant le niveau le plus élevé de désignation ou de classification des pièces jointes tel qu'indiqué dans la Liste de vérification des exigences à la sécurité (LVERS).

3. EXIGENCES MINIMALES DE SÉCURITÉ DES TI

3.1. Vérification de la conformité aux politiques de sécurité des TI

Le MDN se réserve le droit d'inspecter les installations de {Nom de l'entrepreneur} à une fréquence établie par le coordonnateur Ministère de la sécurité des TI. Ces inspections visent à vérifier la conformité des installations aux normes et aux politiques du gouvernement du Canada concernant les exigences de prévention, de détection, de réaction et de reprise contenues dans la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*.

3.2. Conformité aux politiques du gouvernement du Canada

Toutes les opérations relatives aux TI liées à la prévention, à la détection, à l'intervention, et à la récupération des incidents de la sécurité des TI doivent respecter les sections 16 à 18 dans la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*.

3.2.1. Prévention

Les mesures de prévention garantissent la confidentialité, l'intégrité ainsi que la disponibilité de l'information et des biens de TI.

3.2.1.1. Sécurité des lieux visés par les TI

Le matériel utilisé pour le traitement des renseignements protégés/classifiés, doit être autonome ou une partie d'un réseau autonome autorisé désigné pour le stockage et le traitement de jusqu'à, y compris le niveau de Secret et réservé aux canadiens, Secret de l'OTAN, et Secret étranger des données liées au contrat situé dans une zone {Type de zone} telle que définie dans la *Norme opérationnelle sur la sécurité matérielle* du Secrétariat du Conseil du Trésor du Canada (SCT). Ce réseau autonome ne doit servir que pour traiter et de stocker de l'information relative aux contrats avec le MDN et aucun autre client ou partie.

3.2.1.2. Cryptographie, sécurité réseau et défense périmétrique

Le stockage électronique de jusqu'à et y compris le niveau de Secret et réservé aux canadiens, Secret de l'OTAN, et Secret étranger des données liées à ce contrat doit être inclus dans un environnement des TI approuvé par la DSIC. La transmission électronique de l'information protégée A doit être cryptée lorsqu'elle est appuyée par une évaluation de la menace et des risques. Cependant, les informations protégées B et supérieures doivent être cryptées. Pour les informations protégées B et supérieures, le {Nom de l'entrepreneur} doit séparer leurs réseaux respectifs dans des zones de sécurité des TI et mettre en œuvre des mesures de sécurité de

périmètre et de sécurité de réseau. Le Centre de la sécurité des télécommunications Canada (CSTC) fournit les directives ITSG-38 et ITSG-22 sur ce sujet spécifique. De plus, l'entrepreneur / fournisseur doit appliquer un contrôle strict de tous les accès à la zone protégée où les informations associées à ce contrat réside. Des protections de défense de périmètre de réseau (par exemple pare-feu, routeurs) doivent être utilisées pour assurer la médiation de tout le trafic et pour protéger les serveurs accessibles à partir d'Internet. Le {Nom de l'entrepreneur} doit utiliser la technologie de cryptage approuvée par le CSTC pour assurer la confidentialité, l'intégrité, l'authentification et la non-répudiation. Le principe du «besoin de savoir» doit toujours être appliqué pour les informations sensibles et la transmission doit être limitée uniquement aux destinataires approuvés par le DSIC.

3.2.1.3. Stockage et élimination des supports de TI

Tous les matériaux tel que les CD et les DVD, les disques à mémoire flash, les clés USB, les disques durs de poste de travail, l'espace disque de serveur, les bandes de sauvegarde et les autres dispositifs servant au traitement ou au stockage de renseignements classifiés doivent être identifiés et détaillés par désignation ou classification, restriction relative à la diffusion, modèle et numéro de série pour les disques durs, et par désignation ou classification, restriction relative à la diffusion et un numéro d'identification unique pour tous autres supports ou dispositifs qui ne peuvent pas être identifiés par le modèle ou le numéro de série. Ils doivent être conservés et adéquatement rangés ou éliminés par le chef de projet du MDN en cas de défaillance et de remplacement de l'équipement, ou à la résiliation du contrat. Toute destruction de dispositifs ou de matériel doit être autorisée à l'avance par le chef de projet du MDN.

Il faut fournir la liste de l'équipement et des supports utilisés au chef de projet du MDN. De plus, seuls l'équipement et les supports identifiés, détaillés et dont il existe une trace documentaire peuvent être employés pour le traitement de renseignements protégés/classifiés relatifs aux contrats avec le MDN.

Si l'équipement nécessite une maintenance ou un soutien technique ou s'il doit être remplacé, le matériel informatique associé au traitement et au stockage des renseignements protégés/classifiés ne peut pas être confié à un fournisseur externe.

3.2.1.4. Autorisation et contrôle de l'accès

{Nom de l'entrepreneur} doit fournir au chef de projet du MDN la liste de toutes les personnes ayant accès aux renseignements protégés/classifiés devant être traités pour le Ministère, ainsi que ses politiques et ses procédures en vigueur visant l'élargissement de cet accès à d'autres ou sa restriction.

Selon le principe du « droit d'accès minimal », {Nom de l'entrepreneur} doit limiter l'accès au minimum nécessaire pour l'accomplissement des tâches.

3.2.1.5. Informatique mobile et télétravail

Puisqu'une configuration en réseau autonome est exigée, il n'est pas nécessaire de fournir des directives concernant l'informatique mobile et le télétravail. Cependant, les renseignements

protégés/classifiés relatifs aux contrats conclus avec le MDN *ne peuvent être traités que* dans les lieux pour lesquels il y a eu validation par DSIC.

3.2.1.6. Sécurité relative aux émanations

{Nom de l'entrepreneur} doit respecter les politiques de sécurité des émissions (EMSEC) du gouvernement. Cela comprend, sans s'y limiter, la considération à la fois de l'utilisation d'équipements certifiés TEMPEST et du développement et de la mise en œuvre de politiques d'utilisation des communications sans fil spécifiques aux installations.

3.2.1.7. Câblage des moyens de télécommunication

L'accès au câblage utilisé pour l'interconnexion des dispositifs utilisés pour le traitement / la gestion / l'entreposage des informations sensibles au MDN doit être contrôlé et surveillé afin d'empêcher une connexion accidentelle ou délibérée à tout autre réseau ou infrastructure.

3.2.1.8. Intégrité des logiciels et mesures de sécurité

{Nom de l'entrepreneur} doit s'assurer que ses systèmes d'exploitation et que ses logiciels d'application utilisés pour le traitement de renseignements protégés/classifiés du MDN sont conformes aux exigences du gouvernement du Canada. Les correctifs logiciels pour toutes les applications et tous les services fonctionnant sur l'équipement utilisé pour stocker, gérer ou traiter des informations sensibles au MDN doivent être tenus à jour et gérés par un processus de gestion de configuration défini.

3.2.1.9. Programmes malveillants

Puisque les systèmes traitant les renseignements protégés/classifiés sont isolés (système autonome ou en réseau autonome), le risque qu'ils soient exposés à des programmes malveillants comme des virus, des chevaux de Troie ou des vers est peu élevé. Cependant, sans l'application des procédures visant l'implantation de nouveau matériel ou l'utilisation de nouveaux renseignements, ils restent vulnérables. Par conséquent, {Nom de l'entrepreneur} doit installer et utiliser un logiciel antivirus et le mettre à jour régulièrement ainsi que balayer les fichiers électroniques provenant de systèmes externes.

3.2.2. Détection

Il faut être en mesure de détecter les menaces à la sécurité de l'environnement où sont traités les renseignements protégés/classifiés du MDN. Des sources comme des journaux (Observateur d'événements), des logiciels antivirus et d'autres outils de surveillance de systèmes sont utiles même si les systèmes en question sont isolés. Par conséquent, {Nom de l'entrepreneur} doit implémenter une capacité de détecter des problèmes comme l'accès non autorisé, les pannes de systèmes ou de services imprévues ou les changements non autorisés apportés au matériel informatique, aux micrologiciels ou aux logiciels.

3.2.3. Réaction and reprise

3.2.3.1. Réaction aux incidents

Selon la Politique sur la sécurité du gouvernement, les ministères doivent mettre en place des mesures permettant de réagir efficacement aux incidents de sécurité et de communiquer rapidement avec les ministères directeurs désignés à ce sujet. De la même façon, le MDN exige que {Nom de l'entrepreneur} ait un processus de réaction aux incidents et un document connexe. Les détails du processus de réponse aux incidents doivent être fournis dans un document au chef de projet du MDN pour examen et approbation.

3.2.3.2. Déclaration d'incidents

Il est extrêmement important d'aviser le chef de projet du MDN de tous les incidents de sécurité concernant les installations et le matériel utilisé pour traiter et stocker les renseignements protégés/classifiés du MDN relatifs aux contrats avec le MDN.

{Nom de l'entrepreneur} doit déclarer tout incident de sécurité au chef de projet du MDN identifié ci-dessous avant 1200 heures le lendemain du jour où un incident de sécurité a été détecté ou signalé.

3.2.3.3. Reprise

La reprise des systèmes et la récupération de l'information est très importante dans les environnements de TI. Le MDN exige que {Nom de l'entrepreneur} démontre sa capacité à gérer la reprise des systèmes en fournissant des documents relatifs aux politiques de sauvegarde de systèmes et de serveurs (comme les processus utilisés, les tests de restauration, les périodes de rétention et l'emplacement de supports de sauvegarde) pour l'équipement utilisé dans le traitement des renseignements protégés/classifiés du MDN. Les détails des mesures de protection doivent être fournis dans un document au chef de projet du MDN pour examen et approbation.