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 0A1 / Noyau 0A1
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

Revision to a Request for a Standing Offer

Révision à une demande d'offre à commandes

National Individual Standing Offer (NISO)

Offre à commandes individuelle nationale (OCIN)

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

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

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Communication Procurement Directorate/Direction de l'approvisionnement en communication
360 Albert St./ 360, rue Albert
12th Floor / 12ième étage
Ottawa
Ontario
K1A 0S5

Title - Sujet
ELECTRONIC PUBLISHING

Solicitation No. - N° de l'invitation	Date
19294-090124/A	2013-02-21
Client Reference No. - N° de référence du client	**Amendment No. - N° modif.**
19294-9-0124	005
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
cw013.19294-090124	

GETS Reference No. - N° de référence de SEAG
PW-$$CW-013-61970

Date of Original Request for Standing Offer
Date de la demande de l'offre à commandes originale 2013-01-17

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2013-03-07

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Papadatos, Tasia	cw013
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 990-6690 ( )	( ) -

Delivery Required - Livraison exigée

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Security - Sécurité
This revision does not change the security requirements of the Offer.
Cette révision ne change pas les besoins en matière de sécurité de la présente offre.

Instructions: See Herein

Instructions: Voir aux présentes

Acknowledgement copy required / Accusé de réception requis	Yes - Oui	No - Non
	☐	☐

The Offeror hereby acknowledges this revision to its Offer.
Le proposant constate, par la présente, cette révision à son offre.

Signature **Date**

Name and title of person authorized to sign on behalf of offeror. (type or print)
Nom et titre de la personne autorisée à signer au nom du proposant.
(taper ou écrire en caractères d'imprimerie)

For the Minister - Pour le Ministre

Canada

The purpose of this amendment is to provide the Security Requirement Check Lists for Protected and Secret.

All other terms and conditions of the Request for Standing Offer remain the same.

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
19294-090124
Security Classification / Classification de sécurité

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: **Justice Canada**	2. Branch or Directorate / Direction générale ou Direction: IMB / TSD
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
Evidence conversion and publishing services (up to and including Protected-B level)

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 ☑ Kg	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) ☐

DOJ - SSEMD

Security Classification / Classification de sécurité
SN 2011 1 8 0 4

Canada

MJ - DSSGU

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
19294-090124
Security Classification / Classification de sécurité

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
19294-090124
Security Classification / Classification de sécurité

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		✓		X												
Production																
IT Media / Support TI		✓		X												
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
19294-090124 B
Security Classification / Classification de sécurité

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: **Department of Justice Canada**	2. Branch or Directorate / Direction générale ou Direction: IMB / TSD
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
Evidence conversion and publishing services (up to and including the Secret Level).

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

Canada	NATO / OTAN	Foreign / Étranger
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

Canada	NATO	Foreign / Étranger
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
19294-090124 1
Security Classification / Classification de sécurité

1

PART A (continued) / PARTIE A (suite)

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

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☐ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☑ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No ☑ / Yes ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? — Non ☑ / Oui ☐
If Yes, will unscreened personnel be escorted? — No ☐ / Yes ☐
Dans l'affirmative, le personnel en question sera-t-il escorté? — Non ☐ / Oui ☐

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No ☐ / Yes ☑
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ / Oui ☑

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

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No ☑ / Yes ☐
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? — Non ☑ / Oui ☐

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No ☐ / Yes ☑
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ / Oui ☑

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
19294-090124 B
Security Classification / Classification de sécurité

1

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).

CONTRACT

[INSERT CONTRACTOR NAME], hereinafter referred to as the “Contractor”

IT Security

Processing of Protected Information
Department of Justice Canada
December 2010

Version: 1.0 FINAL
2011-03-08

Revision History	Version	Author	Description
2010-12-10	0.1	Duane Doucette	First draft of this document.
2011-02-24	0.2	Duane Doucette	Incorporated comments and questions by Pat O'Rourke.
2011-03-01	0.3	Duane Doucette	Incorporated changes indicted by Pat O'Rourke and Linda Blue.
2011-03-03	0.4	Duane Doucette	Incorporated changes indicted by Pat O'Rourke and Linda Blue.
2011-03-08	1.0 FINAL	Duane Doucette	Incorporated changes indicted by Linda Blue.

CONTENTS

1. INTRODUCTION

This document outlines the federal Department of Justice's (Justice) Information Technology (IT) Security requirements for the processing of protected data up to and including the level of Protected B (PB). 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 safeguards required in order that the processing of PB information be approved by the Department's IT Security Coordinator (ITSC), in addition to the adherence of all safeguards required by the Canadian Industrial Security Directorate (CISD).

Security is based upon layers of protection; that is, in order for the requirements of the IT Security (ITS) 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 and ITS related Standards must exist prior to the implementation of ITS safeguards.

2. MANDATORYPREREQUISITES

2.1. PWGSC Validation for Physical Security

The application of the security safeguards listed in this document are based on the *mandatory requirement* that the physical premises have been inspected, certified and accredited to process and store PB information by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services. The Departmental Security Officer's (DSO) office will validate the certification and notify the ITSC.

A CISD Field Industrial Security Officer (FISO) will perform a bi-annual inspection to ensure that premises PWGSC certification is maintained.

2.2. Personnel Security

All personnel who have access to the material being processed must hold valid Government of Canada security clearance at the appropriate level (dictated by the sensitivity of the material) and have the "*need to know*".

The Department of Justice has the option to request the contractor to attend a Security/IT briefing session.

2.3. Information Security

All hard copy documents and other media formats 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 classification as provided by Justice. Any covering letter, transmittal form or circulation slip will be marked to indicate the highest level of classification of the attachments.

Transportation of information associated with this contract into or out of the physical premises must adhere to RCMP G1-009 "*Transport and Transmittal of Protected and Classified Information*".

2.4. Security Policy Compliance Monitoring

On a frequency to be determined by the Safety, Security and Emergency Management Division (SSEMD), the Department of Justice retains the right to conduct inspections of the contractor's facility to ensure compliance with Government of Canada standards and policies with respect to the handling, storage and processing of protected information.

3. MINIMUM IT SECURITY REQUIREMENTS

3.1. IT Security Policy Compliance and Monitoring

On a frequency to be determined by Technology Services Division/Information Technology Security, the Department of Justice retains the right to conduct inspections of the contractor's 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 of Canada Policies

All information technology related operations must adhere to the overall requirements outlined in the *Operational Security Standard: Management of Information Technology Security*. Specifically, sections 16-18 referring to prevention, detection, response and recovery.

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 contractor will provide the Department of Justice ITSC with the list of physical safeguards which are implemented in the facility which is used to process and store PB information. All equipment processing PB information is to reside in an operations zone as per the RCMP G1-026 "*Guide to the Application of Physical Security Zones*".

The equipment within the operations zone, which is used to process the PB information, must be either standalone, or connected to an *adequately protected*[1] network. In addition, if PB-rated information is contained on the contractor's production network, that network must be certified

[1] A network which has MITS safeguards in place.

and accredited to the level of PB and access to Justice-related information must be restricted to individuals working with the data, who have the required clearance and the need-to-know.

If PB-rated information is to be transmitted, through electronic mail, external to the PB certified and accredited network, all PB content (body or attachment) must be encrypted according to the specifications in ITSA-11d (GoC PKI is adequate).

The use of wireless technology for the processing of PB information is *prohibited.*

3.2.1.2 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 PB information must be identified and itemized by model and serial number for hard disks, and by label for any other media which cannot be identified by model or serial number. These devices or material must be retained and properly wiped or sanitized in a manner adhering to CSEC *ITSG-06: Clearing And Declassifying Electronic Data Storage Devices* upon termination of the final contract.

The contractor must provide the Department of Justice ITSC with a 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 PB information associated with Department of Justice contracts.

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

3.2.1.3 Authorization and Access Control

The contractor must provide the Department of Justice ITSC with a list of all individuals who have access to the PB information being processed for the Department, along with the contractor's 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 must provide only the minimum access required for individuals to perform their duties.

3.2.1.4 Mobile Computing and Teleworking

Mobile computing and teleworking are *prohibited.* Laptops or any removable media, if used, containing PB, information *may not* be removed from the contractor's CISD-inspected site without the written approval of the Department of Justice DSO.

3.2.1.5 Emanations Security

The *Operational Security Standard: Management of Information Technology Security* states that organizations *should* use TEMPEST protection for Top Secret and Protected C information when justified by a Threat and Risk Assessment; therefore, TEMPEST equipment need not be considered unless otherwise required by the CISD.

3.2.1.6 Telecommunications Cabling

It is important to control and monitor access to telecommunications wiring, spaces and pathways to avoid inadvertent or deliberate connection to any other network.

3.2.1.7 Software Integrity and Security Configuration

The contractor must configure the security of their operating systems and application software being used to process PB information in accordance with security best practices (such as the Microsoft Security Compliance Toolkits for servers and clients, CSE or NIST documentation). The contractor must implement safeguards to harden servers and workstations processing PB information, and detail that information in a document to be delivered to the Department of Justice ITSC.

3.2.1.8 Malicious Code

In order to protect systems and information from malicious code such as viruses, trojan horses, and network worms, procedures for introducing new equipment or information into the environment must be documented and followed. In addition to network safeguards such as NIDS and firewall technology, the contractor must install, use and regularly update antivirus and malware detection 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 PB information. It is useful to use sources such as system logs, virus protection software and other system tools to monitor systems. In order to adequately protect information there must exist the ability to detect activity such as unauthorized access, unplanned disruption of systems or services or unauthorized changes to system hardware, firmware, or software. Detection mechanisms which are used by the contractor must be documented and provided to the Department of Justice ITSC.

3.2.3 Response and Recovery

3.2.3.1 Incident Response

The Policy on Government Security 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, the Department requires the contractor to have a documented incident response process. All documentation pertaining to incident response must be provided to the Department of Justice ITSC.

3.2.3.2 Incident Reporting

It is paramount that the Department of Justice DSO and ITSC are made aware of any security-related incidents with respect to the facilities and equipment used to process and store PB information associated with Department of Justice contracts.

The contractor must report any security-related incidents to the Department of Justice DSO and ITSC within *two hours* of an incident being detected or reported.

3.2.3.3 Recovery

The ability to recover systems and information is extremely important in any IT environment. The Department of Justice requires the contractor 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). This documentation shall be forwarded to the Department of Justice ITSC.