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

L’objectif de cette modification est d’ajouter les deux Listes de Vérification des Exigences relatives à la Sécurité (Protégé et Secret).

Toutes les autres termes et conditions demeurent inchangées

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).

CONTRAT N^{O}

[INSÉRER LE NOM DE L'ENTREPRENEUR], ci-après appelé l'« entrepreneur »

Sécurité des TI

Traitement des renseignements protégés
Ministère de la Justice Canada
Décembre 2012

Version : 1.0 FINALE
2011-03-08

Historique des révisions	Version	Auteur	Description
2010-12-10	0.1	Duane Doucette	Première ébauche du présent document
2011-02-24	0.2	Duane Doucette	Intégration des commentaires et questions de Pat O'Rourke.
2011-03-01	0.3	Duane Doucette	Intégration des changements indiqués par Pat O'Rourke et Linda Blue.
2011-03-03	0.4	Duane Doucette	Intégration des changements indiqués par Pat O'Rourke et Linda Blue.
2011-03-08	1.0 Finale	Duane Doucette	Intégration des changements indiqués par Linda Blue

CONTENU

1. INTRODUCTION

Le présent document décrit les exigences de sécurité pour les technologies de l'information (TI) du ministère de la Justice du Canada relativement au traitement des données protégées de niveau « Protégé B » ou 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 B soit approuvé par le coordonnateur de la sécurité des TI du Ministère, ainsi que toutes les mesures de sécurité auxquelles la Direction de la sécurité industrielle canadienne (DSIC) exigent de se conformer.

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 aux normes connexes de sécurité pour les TI doivent avoir été mises en application avant la mise en œuvre d'exigences de sécurité pour les TI.

2. EXIGENCES PRÉALABLES OBLIGATOIRES

2.1. Validation de la sécurité des lieux par TPSGC

L'application des mesures de protection énoncées dans ce document est conditionnelle à l'inspection et à la certification *obligatoires* des lieux en vue du traitement et du stockage de renseignements protégés B par la DSIC du ministère des Travaux publics et des Services gouvernementaux. Le bureau de l'agent de sécurité du ministère (ASM) valide ensuite la certification et en avise le coordonnateur de la sécurité des TI.

Un agent régional de la sécurité industrielle (ARSI) de la DSIC inspecte les lieux deux fois par année pour vérifier si la certification accordée par TPSGC continue de s'y appliquer.

2.2. Sécurité du personnel

Tous les membres du personnel ayant accès aux données traitées doivent avoir une autorisation de sécurité du gouvernement du Canada valide pour le niveau approprié (selon la nature plus ou moins délicate de l'information) ainsi que le « besoin de savoir ».

Le ministère de la Justice peut demander à l'entrepreneur de suivre un atelier de d'information sur la sécurité des TI.

2.3. Sécurité de l'information

Les documents en version papier et sur d'autres supports doivent être manipulés et transportés conformément aux directives du gouvernement du Canada. Il faut y indiquer le niveau de classification de sécurité applicable selon le ministère de la Justice. Les lettres et les formules d'accompagnement ainsi que les bordereaux de circulation doivent être annotés de manière à indiquer le niveau le plus élevé de classification des pièces jointes.

La circulation de l'information relative au présent contrat à l'intérieur et à l'extérieur des lieux doit respecter les exigences énoncées dans le document G1-009 de la Gendarmerie royale du Canada (GRC), intitulé *Transport et transmission de renseignements protégés ou classifiés*.

2.4. Vérification de la conformité aux politiques de sécurité

Le ministère de la Justice se réserve le droit d'inspecter les installations de l'entrepreneur à une fréquence établie selon la Division de la sûreté, de la sécurité et de la gestion des urgences. Ces inspections visent à vérifier la conformité des installations aux normes et aux politiques du gouvernement du Canada concernant la manipulation, le stockage et le traitement de renseignements classifiés.

3. EXIGENCES MINIMALES DE SÉCURITÉ DES TI

3.1. Vérification de la conformité aux politiques de sécurité des TI
3.2.

Le ministère de la Justice se réserve le droit d'inspecter les installations de l'entrepreneur à une fréquence établie par la Division des services technologiques ou la Direction de la sécurité de la technologie de l'information. 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.*

1.
2.
2.1.

3.2. Conformité aux politiques du gouvernement du Canada

Les activités relatives aux TI doivent être conformes aux exigences décrites dans la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* et, en particulier, aux points 16 à 18 de ce même document, où il est question de prévention, de détection, de réaction et de reprise.

1
2
3
3.1
3.2

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

L'entrepreneur fournira au coordonnateur de la sécurité des TI du ministère de la Justice la liste des mesures de prévention mise en œuvre pour protéger les lieux voués au traitement et au stockage des renseignements protégés B. Le matériel servant au traitement de ces renseignements doit être placé dans une zone d'opération aux termes du document G1-026 de la GRC, intitulé *Guide pour l'établissement des zones de sécurité matérielle*.

Le matériel des zones d'opération, utilisé pour le traitement des renseignements protégés B, doit être autonome ou branché à un *réseau adéquatement protégé*[1]. En outre, si le réseau de production de l'entrepreneur contient des renseignements protégés B, ce réseau doit être certifié et accrédité au niveau protégé B, et l'accès aux renseignements liés au ministère de la Justice doit être restreint aux personnes qui utilisent les données, qui possèdent les attestations de sécurité nécessaires et qui ont « besoin de savoir ».

Si des renseignements cotés protégés B doivent être transis par une messagerie électronique ne faisant pas partie du réseau certifié et accrédité, tout le contenu protégé B (le corps du message et les pièces jointes) doit être encrypté conformément aux spécifications de l'Alerte de sécurité des technologies de l'information (ITSA) 11D (l'Infrastructure à clés publiques du gouvernement convient).

Il est interdit d'utiliser la technologie sans fil pour le traitement de renseignements protégés B.

3.2.1.2 Stockage et élimination des supports de TI

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 protégés B doivent être identifiés et détaillés par modèle (et par numéro de série pour les disques durs), ou, lorsque c'est impossible, par étiquette. Ils doivent être conservés et adéquatement rangés ou éliminés

[1] Un réseau comprenant des protections de GSTI.

conformément à la directive ITSG-06 – Effacement et déclassification des supports d'information électroniques du CSTC à la résiliation du contrat final.

L'entrepreneur doit fournir la liste de l'équipement et des supports utilisés au coordonnateur de la sécurité des TI du ministère de la Justice. 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 B relatifs aux contrats avec le Ministère.

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 B ne peut pas être confié à un fournisseur externe.

3.2.1.3 Autorisation et contrôle de l'accès

L'entrepreneur doit fournir au coordonnateur de la sécurité des TI du ministère de la Justice la liste de toutes les personnes ayant accès aux renseignements protégés B devant être traités pour le Ministère, ainsi que ses politiques et ses procédures en vigueur visant l'élargissement de cet accès à d'autres et les procédures suivies au moment où une personne se voit retirer cet accès.

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

3.2.1.4 Informatique mobile et télétravail

L'informatique mobile et le télétravail sont interdits. Les ordinateurs portatifs ou les supports médias amovibles contenant des renseignements protégés B ne peuvent être retirés des installations de l'entrepreneur inspectés par la DSIC sans l'approbation écrite de l'ASM du ministère de la Justice.

3.2.1.5 Sécurité relative aux émanations

Selon la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*, les organismes devraient utiliser la protection TEMPEST pour les renseignements « Très secret » ou « Protégé C » lorsqu'une EMR le justifie. Par conséquent, il ne faut pas utiliser l'équipement TEMPEST à moins que la DSIC l'exige.

3.2.1.6 Câblage des moyens de télécommunication

Il est important de contrôler et de surveiller l'accès au câblage, aux espaces et aux chemins d'accès de télécommunication pour éviter toute connexion, intentionnelle ou non, à un autre réseau.

3.2.1.7 Intégrité des logiciels et mesures de sécurité

L'entrepreneur doit s'assurer de configurer ses systèmes d'exploitation et ses logiciels d'application utilisés pour le traitement de renseignements protégés B conformément aux meilleures pratiques concernant la sécurité (comme les trousses sur la conformité en matière de sécurité de Microsoft pour les serveurs et les clients et la documentation du Centre de la sécurité des télécommunications et de l'Institut national des normes et des technologies). L'entrepreneur doit mettre en œuvre des mesures de protection pour « renforcer » ses serveurs et ses postes de travail liés au traitement de renseignements protégés B et les expliquer en détail dans un document à fournir au coordonnateur de la sécurité des TI du ministère de la Justice.

3.2.1.8 Code malveillant

Afin de protéger les systèmes et les renseignements contre des programmes malveillants comme des virus, des chevaux de Troie ou des vers, il faut mettre en place et documenter des procédures visant l'implantation de nouveau matériel ou l'utilisation de nouveaux renseignements. En plus de mesures de protection pour les réseaux comme le Système de détection des intrusions sur réseau et la technologie pare-feu, 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 est important d'être en mesure de détecter les menaces à la sécurité dans l'environnement opérationnel où sont traités les renseignements protégés B. Des sources comme des journaux, des logiciels antivirus et d'autres outils de surveillance de systèmes sont utiles. Pour protéger l'information de manière appropriée, il faut d'abord être capable 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. Les mesures de détection mises en œuvre par l'entrepreneur doivent être documentées et fournies au coordonnateur de la sécurité des TI du Ministère de la Justice.

3.2.3 Réaction et 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 Ministère exige que l'entrepreneur ait un processus de réaction aux incidents et un document connexe. La documentation relative à la réaction aux incidents doit être fournie au coordonnateur de la sécurité des TI du ministère de la Justice.

3.2.3.2 Déclaration d'incidents

Il est extrêmement important d'aviser l'ASM et le coordonnateur de la sécurité des TI du ministère de la Justice d'un incident de sécurité concernant les installations et le matériel utilisé pour traiter et stocker les renseignements protégés B relatifs aux contrats avec le Ministère.

L'entrepreneur doit déclarer tout incident de sécurité à l'ASM et au coordonnateur de la sécurité des TI du ministère de la Justice dans les *deux heures* suivant sa détection ou son signalement.

3.2.3.3 Reprise

La reprise des systèmes et la récupération de l'information est très importante dans les environnements de TI. Le ministère de la Justice exige que 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). Cette documentation doit être transmise au coordonnateur de la sécurité des TI du ministère de la Justice.