



| |
|--|
| Contract Number / Numéro du contrat |
| 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 | 2. Branch or Directorate / Direction générale ou Direction |
| 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

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? No / Non Yes / Oui
(Specify the level of access using the chart in Question 7. c) / (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. / Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. 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 <input type="checkbox"/> | NATO / OTAN <input type="checkbox"/> | Foreign / Étranger <input type="checkbox"/> |
|---------------------------------|--------------------------------------|---|

7. b) Release restrictions / Restrictions relatives à la diffusion

| | | |
|---|--|--|
| No release restrictions / Aucune restriction relative à la diffusion <input type="checkbox"/> Not releasable / À ne pas diffuser <input type="checkbox"/> Restricted to: / Limité à: <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays: | All NATO countries / Tous les pays de l'OTAN <input type="checkbox"/> Restricted to: / Limité à: <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays: | No release restrictions / Aucune restriction relative à la diffusion <input type="checkbox"/> Restricted to: / Limité à: <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays: |
|---|--|--|

7. c) Level of information / Niveau d'information

| | | |
|---|--|---|
| PROTECTED A / PROTÉGÉ A <input type="checkbox"/> | NATO UNCLASSIFIED / NATO NON CLASSIFIÉ <input type="checkbox"/> | PROTECTED A / PROTÉGÉ A <input type="checkbox"/> |
| PROTECTED B / PROTÉGÉ B <input type="checkbox"/> | NATO RESTRICTED / NATO DIFFUSION RESTREINTE <input type="checkbox"/> | PROTECTED B / PROTÉGÉ B <input type="checkbox"/> |
| PROTECTED C / PROTÉGÉ C <input type="checkbox"/> | NATO CONFIDENTIAL / NATO CONFIDENTIEL <input type="checkbox"/> | PROTECTED C / PROTÉGÉ C <input type="checkbox"/> |
| CONFIDENTIAL / CONFIDENTIEL <input type="checkbox"/> | NATO SECRET / NATO SECRET <input type="checkbox"/> | CONFIDENTIAL / CONFIDENTIEL <input type="checkbox"/> |
| SECRET / SECRET <input type="checkbox"/> | COSMIC TOP SECRET / COSMIC TRÈS SECRET <input type="checkbox"/> | SECRET / SECRET <input type="checkbox"/> |
| TOP SECRET / TRÈS SECRET <input type="checkbox"/> | | TOP SECRET / TRÈS SECRET <input type="checkbox"/> |
| TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) <input type="checkbox"/> | | TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) <input type="checkbox"/> |

| |
|--|
| Security Classification / Classification de sécurité |
|--|



| |
|--|
| Contract Number / Numéro du contrat |
| 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 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

| | | | |
|---|---|---|--|
| <input type="checkbox"/> RELIABILITY STATUS COTE DE FIABILITÉ | <input type="checkbox"/> CONFIDENTIAL CONFIDENTIEL | <input type="checkbox"/> SECRET SECRET | <input type="checkbox"/> TOP SECRET TRÈS SECRET |
| <input type="checkbox"/> TOP SECRET- SIGINT TRÈS SECRET - SIGINT | <input type="checkbox"/> NATO CONFIDENTIAL NATO CONFIDENTIEL | <input type="checkbox"/> NATO SECRET NATO SECRET | <input type="checkbox"/> COSMIC TOP SECRET COSMIC TRÈS SECRET |
| <input type="checkbox"/> SITE ACCESS ACCÈS AUX EMBLEMES | | | |

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?
 Dans l'affirmative, le personnel en question sera-t-il escorté? No Yes
 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



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 | | | CONFIDENTIAL / CONFIDENTIEL | SECRET | TOP SECRET / TRÈS SECRET |
| | | | | | | | | | | | A | B | C | | | |
| 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? No Yes
 La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE? Non Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifiez 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? No Yes
 La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE? Non 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, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquez qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).



| |
|--|
| Contract Number / Numéro du contrat |
| Security Classification / Classification de sécurité |

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 |
| Telephone No. - N° de téléphone | Facsimile No. - N° de télécopieur | E-mail address - Adresse courriel | Date |
| 14. Organization Security Authority / Responsable de la sécurité de l'organisme | | | |
| Name (print) - Nom (en lettres moulées) | | Title - Titre | Signature |
| Telephone No. - N° de téléphone | Facsimile No. - N° de télécopieur | E-mail address - Adresse courriel | Date |
| 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? | | | <input type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui |
| 16. Procurement Officer / Agent d'approvisionnement | | | |
| Name (print) - Nom (en lettres moulées) | | Title - Titre | Signature |
| Telephone No. - N° de téléphone | Facsimile No. - N° de télécopieur | E-mail address - Adresse courriel | Date |
| 17. Contracting Security Authority / Autorité contractante en matière de sécurité | | | |
| Name (print) - Nom (en lettres moulées) | | Title - Titre | Signature |
| Telephone No. - N° de téléphone | Facsimile No. - N° de télécopieur | E-mail address - Adresse courriel | Date |

| |
|--|
| Security Classification / Classification de sécurité |
|--|

Instructions for completion of a Security Requirements Check List (SRCL)

The instruction sheet should remain attached until Block #17 has been completed.

GENERAL - PROCESSING THIS FORM

The project authority shall arrange to complete this form.

The organization security officer shall review and approve the security requirements identified in the form, in cooperation with the project authority.

The contracting security authority is the organization responsible for ensuring that the suppliers are compliant with the security requirements identified in the SRCL.

All requisitions and subsequent tender / contractual documents including subcontracts that contain PROTECTED and/or CLASSIFIED requirements must be accompanied by a completed SRCL.

It is important to identify the level of PROTECTED information or assets as Level "A," "B" or "C," when applicable; however, certain types of information may only be identified as "PROTECTED". No information pertaining to a PROTECTED and/or CLASSIFIED government contract may be released by suppliers, without prior written approval of the individual identified in Block 17 of this form.

The classification assigned to a particular stage in the contractual process does not mean that everything applicable to that stage is to be given the same classification. Every item shall be PROTECTED and/or CLASSIFIED according to its own content. If a supplier is in doubt as to the actual level to be assigned, they should consult with the individual identified in Block 17 of this form.

PART A - CONTRACT INFORMATION

Contract Number (top of the form)

This number must be the same as that found on the requisition and should be the one used when issuing an RFP or contract. This is a unique number (i.e. no two requirements will have the same number). A new SRCL must be used for each new requirement or requisition (e.g. new contract number, new SRCL, new signatures).

1. Originating Government Department or Organization

Enter the department or client organization name or the prime contractor name for which the work is being performed.

2. Directorate / Branch

This block is used to further identify the area within the department or organization for which the work will be conducted.

3. a) Subcontract Number

If applicable, this number corresponds to the number generated by the Prime Contractor to manage the work with its subcontractor.

b) Name and Address of Subcontractor

Indicate the full name and address of the Subcontractor if applicable.

4. Brief Description of Work

Provide a brief explanation of the nature of the requirement or work to be performed.

5. a) Will the supplier require access to Controlled Goods?

*The Defence Production Act (DPA) defines "Controlled Goods" as certain goods listed in the Export Control List, a regulation made pursuant to the *Export and Import Permits Act* (EIPA). Suppliers who examine, possess, or transfer Controlled Goods within Canada must register in the Controlled Goods Directorate or be exempt from registration. More information may be found at www.cgd.gc.ca.*

b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?

The prime contractor and any subcontractors must be certified under the U.S./Canada Joint Certification Program if the work involves access to unclassified military data subject to the provisions of the Technical Data Control Regulations. More information may be found at www.dlis.dla.mil/jcp.

6. Indicate the type of access required

Identify the nature of the work to be performed for this requirement. The user is to select one of the following types:

a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?

The supplier would select this option if they require access to PROTECTED and/or CLASSIFIED information or assets to perform the duties of the requirement.

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.

The supplier would select this option if they require regular access to government premises or a secure work site only. The supplier will not have access to PROTECTED and/or CLASSIFIED information or assets under this option.

c) Is this a commercial courier or delivery requirement with no overnight storage?

The supplier would select this option if there is a commercial courier or delivery requirement. The supplier will not be allowed to keep a package overnight. The package must be returned if it cannot be delivered.

7. Type of information / Release restrictions / Level of information

Identify the type(s) of information that the supplier may require access to, list any possible release restrictions, and if applicable, provide the level(s) of the information. The user can make multiple selections based on the nature of the work to be performed.

Departments must process SRCLs through PWGSC where:

- contracts that afford access to PROTECTED and/or CLASSIFIED foreign government information and assets;
- contracts that afford foreign contractors access to PROTECTED and/or CLASSIFIED Canadian government information and assets; or
- contracts that afford foreign or Canadian contractors access to PROTECTED and/or CLASSIFIED information and assets as defined in the documents entitled Identifying INFOSEC and INFOSEC Release.

a) Indicate the type of information that the supplier will be required to access

Canadian government information and/or assets

If Canadian information and/or assets are identified, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by the Canadian government.

NATO information and/or assets

If NATO information and/or assets are identified, this indicates that as part of this requirement, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by NATO governments. NATO information and/or assets are developed and/or owned by NATO countries and are not to be divulged to any country that is not a NATO member nation. Persons dealing with NATO information and/or assets must hold a NATO security clearance and have the required need-to-know.

Requirements involving CLASSIFIED NATO information must be awarded by PWGSC. PWGSC / CIISD is the Designated Security Authority for industrial security matters in Canada.

Foreign government information and/or assets

If foreign information and/or assets are identified, this requirement will allow access to information and/or assets owned by a country other than Canada.

b) Release restrictions

If **Not Releasable** is selected, this indicates that the information and/or assets are for **Canadian Eyes Only (CEO)**. Only Canadian suppliers based in Canada can bid on this type of requirement. NOTE: If Canadian information and/or assets coexists with CEO information and/or assets, the CEO information and/or assets must be stamped **Canadian Eyes Only (CEO)**.

If **No Release Restrictions** is selected, this indicates that access to the information and/or assets are not subject to any restrictions.

If **ALL NATO countries** is selected, bidders for this requirement must be from NATO member countries only.

NOTE: There may be multiple release restrictions associated with a requirement depending on the nature of the work to be performed. In these instances, a security guide should be added to the SRCL clarifying these restrictions. The security guide is normally generated by the organization's project authority and/or security authority.

c) Level of information

Using the following chart, indicate the appropriate level of access to information/assets the supplier must have to perform the duties of the requirement.

| PROTECTED | CLASSIFIED | NATO |
|-------------|---------------------|-------------------|
| PROTECTED A | CONFIDENTIAL | NATO UNCLASSIFIED |
| PROTECTED B | SECRET | NATO RESTRICTED |
| PROTECTED C | TOP SECRET | NATO CONFIDENTIAL |
| | TOP SECRET (SIGINT) | NATO SECRET |
| | | COSMIC TOP SECRET |

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?

If Yes, the supplier personnel requiring access to COMSEC information or assets must receive a COMSEC briefing. The briefing will be given to the "holder" of the COMSEC information or assets. In the case of a "personnel assigned" type of contract, the customer department will give the briefing. When the supplier is required to receive and store COMSEC information or assets on the supplier's premises, the supplier's COMSEC Custodian will give the COMSEC briefings to the employees requiring access to COMSEC information or assets. If Yes, the Level of sensitivity must be indicated.

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?

If Yes, the supplier must provide the Short Title of the material and the Document Number. Access to extremely sensitive INFOSEC information or assets will require that the supplier undergo a Foreign Ownership Control or Influence (FOCI) evaluation by CIISD.

PART B - PERSONNEL (SUPPLIER)

10. a) Personnel security screening level required

Identify the screening level required for access to the information/assets or client facility. More than one level may be identified depending on the nature of the work. Please note that Site Access screenings are granted for access to specific sites under prior arrangement with the Treasury Board of Canada Secretariat. A Site Access screening only applies to individuals, and it is not linked to any other screening level that may be granted to individuals or organizations.

| RELIABILITY STATUS | CONFIDENTIAL | SECRET |
|--------------------|---------------------|-------------------|
| TOP SECRET | TOP SECRET (SIGINT) | NATO CONFIDENTIAL |
| NATO SECRET | COSMIC TOP SECRET | SITE ACCESS |

If multiple levels of screening are identified, a Security Classification Guide must be provided.

b) May unscreened personnel be used for portions of the work?

Indicating Yes means that portions of the work are not PROTECTED and/or CLASSIFIED and may be performed outside a secure environment by unscreened personnel. The following question must be answered if unscreened personnel will be used:

Will unscreened personnel be escorted?

If No, unscreened personnel may not be allowed access to sensitive work sites and must not have access to PROTECTED and/or CLASSIFIED information and/or assets.

If Yes, unscreened personnel must be escorted by an individual who is cleared to the required level of security in order to ensure there will be no access to PROTECTED and/or CLASSIFIED information and/or assets at the work site.

PART C - SAFEGUARDS (SUPPLIER)

11. INFORMATION / ASSETS

a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information and/or assets on its site or premises?

If Yes, specify the security level of the documents and/or equipment that the supplier will be required to safeguard at their own site or premises using the summary chart.

b) Will the supplier be required to safeguard COMSEC information or assets?

If Yes, specify the security level of COMSEC information or assets that the supplier will be required to safeguard at their own site or premises using the summary chart.

PRODUCTION

c) Will the production (manufacture, repair and/or modification) of PROTECTED and/or CLASSIFIED material and/or equipment occur at the supplier's site or premises?

Using the summary chart, specify the security level of material and/or equipment that the supplier manufactured, repaired and/or modified and will be required to safeguard at their own site or premises.

INFORMATION TECHNOLOGY (IT)

d) Will the supplier be required to use its IT systems to electronically process and/or produce or store PROTECTED and/or CLASSIFIED information and/or data?

If Yes, specify the security level in the summary chart. This block details the information and/or data that will be electronically processed or produced and stored on a computer system. The client department and/or organization will be required to specify the IT security requirements for this procurement in a separate technical document. The supplier must also direct their attention to the following document: Treasury Board of Canada Secretariat - Operational Security Standard: Management of Information Technology Security (MITS).

e) Will there be an electronic link between the supplier’s IT systems and the government department or agency?

If Yes, the supplier must have their IT system(s) approved. The Client Department must also provide the Connectivity Criteria detailing the conditions and the level of access for the electronic link (usually not higher than PROTECTED B level).

SUMMARY CHART

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.

For users completing the form **online** (via the Internet), the Summary Chart is automatically populated by your responses to previous questions.

| PROTECTED | CLASSIFIED | NATO | COMSEC |
|-------------|---------------------|-------------------|--------------|
| PROTECTED A | CONFIDENTIAL | NATO RESTRICTED | PROTECTED A |
| PROTECTED B | SECRET | NATO CONFIDENTIAL | PROTECTED B |
| PROTECTED C | TOP SECRET | NATO SECRET | PROTECTED C |
| | TOP SECRET (SIGINT) | COSMIC TOP SECRET | CONFIDENTIAL |
| | | | SECRET |
| | | | TOP SECRET |

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?

If Yes, classify this form by annotating the top and bottom in the area entitled “Security Classification”.

b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?

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).

PART D - AUTHORIZATION

13. Organization Project Authority

This block is to be completed and signed by the appropriate project authority within the client department or organization (e.g. the person responsible for this project or the person who has knowledge of the requirement at the client department or organization). This person may on occasion be contacted to clarify information on the form.

14. Organization Security Authority

This block is to be signed by the Departmental Security Officer (DSO) (or delegate) of the department identified in Block 1, or the security official of the prime contractor.

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?

A Security Guide or Security Classification Guide is used in conjunction with the SRCL to identify additional security requirements which do not appear in the SRCL, and/or to offer clarification to specific areas of the SRCL.

16. Procurement Officer

This block is to be signed by the procurement officer acting as the contract or subcontract manager.

17. Contracting Security Authority

This block is to be signed by the Contract Security Official. Where PWGSC is the Contract Security Authority, Canadian and International Industrial Security Directorate (CIISD) will complete this block.

Instructions pour établir la Liste de vérification des exigences relatives à la sécurité (LVERS)

La feuille d'instructions devrait rester jointe au formulaire jusqu'à ce que la case 17 ait été remplie.

GÉNÉRALITÉS - TRAITEMENT DU PRÉSENT FORMULAIRE

Le responsable du projet doit faire remplir ce formulaire.

L'agent de sécurité de l'organisation doit revoir et approuver les exigences de sécurité qui figurent dans le formulaire, en collaboration avec le responsable du projet.

Le responsable de la sécurité des marchés est le responsable chargé de voir à ce que les fournisseurs se conforment aux exigences de sécurité mentionnées dans la LVERS.

Toutes les demandes d'achat ainsi que tous les appels d'offres et les documents contractuels subséquents, y compris les contrats de sous-traitance, qui comprennent des exigences relatives à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS doivent être accompagnés d'une LVERS dûment remplie.

Il importe d'indiquer si les renseignements ou les biens PROTÉGÉS sont de niveau A, B ou C, le cas échéant; cependant, certains types de renseignements peuvent être indiqués par la mention « PROTÉGÉ » seulement. Aucun renseignement relatif à un contrat gouvernemental PROTÉGÉ ou CLASSIFIÉ ne peut être divulgué par les fournisseurs sans l'approbation écrite préalable de la personne dont le nom figure à la case 17 de ce formulaire.

La classification assignée à un stade particulier du processus contractuel ne signifie pas que tout ce qui se rapporte à ce stade doit recevoir la même classification. Chaque article doit être PROTÉGÉ et/ou CLASSIFIÉ selon sa propre nature. Si un fournisseur ne sait pas quel niveau de classification assigner, il doit consulter la personne dont le nom figure à la case 17 de ce formulaire.

PARTIE A - INFORMATION CONTRACTUELLE

Numéro du contrat (au haut du formulaire)

Ce numéro doit être le même que celui utilisé sur la demande d'achat et services et devrait être celui utilisé dans la DDP ou dans le contrat. Il s'agit d'un numéro unique (c.-à-d. que le même numéro ne sera pas attribué à deux besoins distincts). Une nouvelle LVERS doit être utilisée pour chaque nouveau besoin ou demande (p. ex. un nouveau numéro de contrat, une nouvelle LVERS, de nouvelles signatures).

1. Ministère ou organisme gouvernemental d'origine

Inscrire le nom du ministère ou de l'organisme client ou le nom de l'entrepreneur principal pour qui les travaux sont effectués.

2. Direction générale ou Direction

Cette case peut servir à fournir plus de détails quant à la section du ministère ou de l'organisme pour qui les travaux sont effectués.

3. a) Numéro du contrat de sous-traitance

S'il y a lieu, ce numéro correspond au numéro généré par l'entrepreneur principal pour gérer le travail avec son sous-traitant.

b) Nom et adresse du sous-traitant

Indiquer le nom et l'adresse au complet du sous-traitant, s'il y a lieu.

4. Brève description du travail

Donner un bref aperçu du besoin ou du travail à exécuter.

5. a) Le fournisseur aura-t-il accès à des marchandises contrôlées?

La *Loi sur la production de défense* (LPD) définit « marchandises contrôlées » comme désignant certains biens énumérés dans la Liste des marchandises d'exportation contrôlée, un règlement établi en vertu de la *Loi sur les licences d'exportation et d'importation* (LLEI). Les fournisseurs qui examinent, possèdent ou transfèrent des marchandises contrôlées à l'intérieur du Canada doivent s'inscrire à la Direction des marchandises contrôlées ou être exemptés de l'inscription. On trouvera plus d'information à l'adresse www.cgp.gc.ca.

b) 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?

L'entrepreneur et tout sous-traitant doivent être accrédités en vertu du Programme mixte d'agrément Etats-Unis / Canada si le travail comporte l'accès à des données militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques. On trouvera plus d'information à l'adresse www.dlis.dla.mil/jcp/.

6. Indiquer le type d'accès requis

Indiquer la nature du travail à exécuter pour répondre à ce besoin. L'utilisateur doit choisir un des types suivants :

a) Le fournisseur et ses employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?

Le fournisseur choisit cette option s'il doit avoir accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS pour accomplir le travail requis.

b) 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.

Le fournisseur choisit cette option seulement s'il doit avoir accès régulièrement aux locaux du gouvernement ou à un lieu de travail protégé. Le fournisseur n'aura pas accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS en vertu de cette option.

c) S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?

Le fournisseur choisit cette option s'il y a nécessité de recourir à un service de messagerie ou de livraison commerciale. Le fournisseur ne sera pas autorisé à garder un colis pendant la nuit. Le colis doit être retourné s'il ne peut pas être livré.

7. Type d'information / Restrictions relatives à la diffusion / Niveau d'information

Indiquer le ou les types d'information auxquels le fournisseur peut devoir avoir accès, énumérer toutes les restrictions possibles relatives à la diffusion, et, s'il y a lieu, indiquer le ou les niveaux d'information. L'utilisateur peut faire plusieurs choix selon la nature du travail à exécuter.

Les ministères doivent soumettre la LVERS à TPSGC lorsque:

- les marchés prévoient l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS étrangers ;
- les marchés prévoient aux entrepreneurs étrangers l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS canadiens; ou
- les marchés prévoient aux entrepreneurs étrangers ou canadiens l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS tels que définis dans les documents intitulés Moyens INFOSEC détermination et Divulgateion de INFOSEC.

a) Indiquer le type d'information auquel le fournisseur devra avoir accès

Renseignements et/ou biens du gouvernement canadien

Si des renseignements et/ou des biens canadiens sont indiqués, le fournisseur aura accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS appartenant au gouvernement canadien.

Renseignements et/ou biens de l'OTAN

Si des renseignements et/ou des biens de l'OTAN sont indiqués, cela signifie que, dans le cadre de ce besoin, le fournisseur aura accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS appartenant à des gouvernements membres de l'OTAN. Les renseignements et/ou les biens de l'OTAN sont élaborés par des pays de l'OTAN ou leur appartiennent et ne doivent être divulgués à aucun pays qui n'est pas un pays membre de l'OTAN. Les personnes qui manient des renseignements et/ou des biens de l'OTAN doivent détenir une autorisation de sécurité de l'OTAN et avoir besoin de savoir.

Les contrats comportant des renseignements CLASSIFIÉS de l'OTAN doivent être attribués par TPSGC. La DSICI de TPSGC est le responsable de la sécurité désigné relativement aux questions de sécurité industrielle au Canada.

Renseignements et/ou biens de gouvernements étrangers

Si des renseignements et/ou des biens de gouvernements étrangers sont indiqués, ce besoin permettra l'accès à des renseignements et/ou à des biens appartenant à un pays autre que le Canada.

b) Restrictions relatives à la diffusion

Si **À ne pas diffuser** est choisi, cela indique que les renseignements et/ou les biens sont **réservés aux Canadiens**. Seuls des fournisseurs canadiens installés au Canada peuvent soumissionner ce genre de besoin. NOTA : Si des renseignements et/ou des biens du gouvernement canadien coexistent avec des renseignements et/ou des biens réservés aux Canadiens, ceux-ci doivent porter la mention **Réservé aux Canadiens**.

Si **Aucune restriction relative à la diffusion** est choisi, cela indique que l'accès aux renseignements et/ou aux biens n'est assujéti à aucune restriction.

Si **Tous les pays de l'OTAN** est choisi, les soumissionnaires doivent appartenir à un pays membre de l'OTAN.

NOTA : Il peut y avoir plus d'une restriction s'appliquant à une demande, selon la nature des travaux à exécuter. Pour ce genre de contrat, un guide de sécurité doit être joint à la LVERS afin de clarifier les restrictions. Ce guide est généralement préparé par le chargé de projet et/ou le responsable de la sécurité de l'organisme.

c) Niveau d'information

À l'aide du tableau ci-dessous, indiquer le niveau approprié d'accès aux renseignements et/ou aux biens que le fournisseur doit avoir pour accomplir les travaux requis.

| PROTÉGÉ | CLASSIFIÉ | NATO |
|-----------|----------------------|---------------------------|
| PROTÉGÉ A | CONFIDENTIEL | NATO NON CLASSIFIÉ |
| PROTÉGÉ B | SECRET | NATO DIFFUSION RESTREINTE |
| PROTÉGÉ C | TRÈS SECRET | NATO CONFIDENTIEL |
| | TRÈS SECRET (SIGINT) | NATO SECRET |
| | | COSMIC TRÈS SECRET |

8. Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?

Si la réponse est Oui, les membres du personnel du fournisseur qui doivent avoir accès à des renseignements ou à des biens COMSEC doivent participer à une séance d'information COMSEC. Cette séance sera donnée au « détenteur autorisé » des renseignements ou des biens COMSEC. Dans le cas des contrats du type « personnel affecté », cette séance sera donnée par le ministère client. Lorsque le fournisseur doit recevoir et conserver, dans ses locaux, des renseignements ou des biens COMSEC, le responsable de la garde des renseignements ou des biens COMSEC de l'entreprise donnera la séance d'information COMSEC aux membres du personnel qui doivent avoir accès à des renseignements ou à des biens COMSEC.

9. Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Si la réponse est Oui, le fournisseur doit indiquer le titre abrégé du document, le numéro du document et le niveau de sensibilité. L'accès à des renseignements ou à des biens extrêmement délicats INFOSEC exigera que le fournisseur fasse l'objet d'une vérification Participation, contrôle et influence étrangers (PCIE) effectuée par la DSICI.

PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Niveau de contrôle de la sécurité du personnel requis

Indiquer le niveau d'autorisation de sécurité que le personnel doit détenir pour avoir accès aux renseignements, aux biens ou au site du client. Selon la nature du travail, il peut y avoir plus d'un niveau de sécurité. Veuillez noter que des cotes de sécurité sont accordées pour l'accès à des sites particuliers, selon des dispositions antérieures prises auprès du Secrétariat du Conseil du Trésor du Canada. La cote de sécurité donnant accès à un site s'applique uniquement aux personnes et n'est liée à aucune autre autorisation de sécurité accordée à des personnes ou à des organismes.

| COTE DE FIABILITÉ | CONFIDENTIEL | SECRET |
|-------------------|----------------------|--------------------|
| TRÈS SECRET | TRÈS SECRET (SIGINT) | NATO CONFIDENTIEL |
| NATO SECRET | COSMIC TRÈS SECRET | ACCÈS AUX EMBLEMES |

Si plusieurs niveaux d'autorisation de sécurité sont indiqués, un guide de classification de sécurité doit être fourni.

b) Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

Si la réponse est Oui, cela veut dire que certaines tâches ne sont pas PROTÉGÉES et/ou CLASSIFIÉES et peuvent être exécutées à l'extérieur d'un environnement sécurisé par du personnel n'ayant pas d'autorisation de sécurité. Il faut répondre à la question suivante si l'on a recours à du personnel n'ayant pas d'autorisation de sécurité :

Le personnel n'ayant pas d'autorisation de sécurité sera-t-il escorté?

Si la réponse est Non, le personnel n'ayant pas d'autorisation de sécurité ne pourra pas avoir accès à des lieux de travail dont l'accès est réglementé ni à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS.

Si la réponse est Oui, le personnel n'ayant pas d'autorisation de sécurité devra être escorté par une personne détenant la cote de sécurité requise, pour faire en sorte que le personnel en question n'ait pas accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS sur les lieux de travail.

PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

11. RENSEIGNEMENTS / BIENS :

a) Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

Si la réponse est Oui, préciser, à l'aide du tableau récapitulatif, le niveau de sécurité des documents ou de l'équipement que le fournisseur devra protéger dans ses installations.

b) Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

Si la réponse est Oui, préciser, à l'aide du tableau récapitulatif, le niveau de sécurité des renseignements ou des biens COMSEC que le fournisseur devra protéger dans ses installations.

PRODUCTION

c) Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

Préciser, à l'aide du tableau récapitulatif, le niveau de sécurité du matériel que le fournisseur fabriquera, réparera et/ou modifiera et devra protéger dans ses installations.

TECHNOLOGIE DE L'INFORMATION (TI)

d) 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?

Si la réponse est Oui, préciser le niveau de sécurité à l'aide du tableau récapitulatif. Cette case porte sur les renseignements qui seront traités ou produits électroniquement et stockés dans un système informatique. Le ministère/organisme client devra préciser les exigences en matière de sécurité de la TI relativement à cet achat dans un document technique distinct. Le fournisseur devra également consulter le document suivant : Secrétariat du Conseil du Trésor du Canada – Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI).

e) Y aura-t-il un lien électronique entre les systèmes informatiques du fournisseur et celui du ministère ou de l'agence gouvernementale?

Si la réponse est Oui, le fournisseur doit faire approuver ses systèmes informatiques. Le ministère client doit aussi fournir les critères de connectivité qui décrivent en détail les conditions et le niveau de sécurité relativement au lien électronique (habituellement pas plus haut que le niveau PROTÉGÉ B).

TABLEAU RÉCAPITULATIF

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.

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.

| PROTÉGÉ | CLASSIFIÉ | NATO | COMSEC |
|-----------|----------------------|---------------------------|--------------|
| PROTÉGÉ A | CONFIDENTIEL | NATO DIFFUSION RESTREINTE | PROTÉGÉ A |
| PROTÉGÉ B | SECRET | NATO CONFIDENTIEL | PROTÉGÉ B |
| PROTÉGÉ C | TRÈS SECRET | NATO SECRET | PROTÉGÉ C |
| | TRÈS SECRET (SIGINT) | COSMIC TRÈS SECRET | CONFIDENTIEL |
| | | | SECRET |
| | | | TRÈS SECRET |

12. a) La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

Si la réponse est Oui, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de

sécurité » au haut et au bas du formulaire.

b) La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

Si la réponse est Oui, classifiez 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).

PARTIE D - AUTORISATION

13. Chargé de projet de l'organisme

Cette case doit être remplie et signée par le chargé de projet pertinent (c.-à-d. la personne qui est responsable de ce projet ou qui connaît le besoin au ministère ou à l'organisme client. On peut, à l'occasion, communiquer avec cette personne pour clarifier des renseignements figurant sur le formulaire.

14. Responsable de la sécurité de l'organisme

Cette case doit être signée par l'agent de la sécurité du ministère (ASM) du ministère indiqué à la case 1 ou par son remplaçant ou par le responsable de la sécurité du fournisseur.

15. Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

Un Guide de sécurité ou un Guide de classification de sécurité sont utilisés de concert avec la LVERS pour faire part d'exigences supplémentaires en matière de sécurité qui n'apparaissent pas dans la LVERS et/ou pour éclaircir certaines parties de la LVERS.

16. Agent d'approvisionnement

Cette case doit être signée par l'agent des achats qui fait fonction de gestionnaire du contrat ou du contrat de sous-traitance.

17. Autorité contractante en matière de sécurité

Cette case doit être signée par l'agent de la sécurité du marché. Lorsque TPSGC est le responsable de la sécurité du marché, la Direction de la sécurité industrielle canadienne et internationale (DSICI) doit remplir cette case.