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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Michael Randall
Les Terrasses de la Chaudière
5th Floor
10 Wellington Street
Gatineau
Quebec
K1A 0S5

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Health Services Project Division (XF)/Division des projets de services de santé (XF)
Terrasses de la Chaudière 5th Floo
10 Wellington Street
Gatineau
Gatineau
K1A 0S5

Title - Sujet Administrative Services	
Solicitation No. - N° de l'invitation 24062-180558/A	**Date** 2018-02-16
Client Reference No. - N° de référence du client 24062-180558	**GETS Ref. No. - N° de réf. de SEAG** PW-$$XF-050-32201
File No. - N° de dossier 050xf.24062-180558	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2018-03-16**	**Time Zone** **Fuseau horaire** Eastern Standard Time EST
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Randall, Michael	**Buyer Id - Id de l'acheteur** 050xf
Telephone No. - N° de téléphone (613) 558-1053 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** TREASURY BOARD OF CANADA, SECRETARIAT 90 Elgin Street OTTAWA Ontario Canada	

Instructions: See Herein

Instructions: Voir aux présentes

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

Canada

LETTER OF INTEREST (LOI)

FOR

Treasury Board of Canada Secretariat (TBS)

Public Service Health Care Plan (PSHCP) Administrative Services Only (ASO) Requirement

Table of Contents

PART I: LETTER OF INTEREST PROCESS

1. INTRODUCTION

1.1 Background of this Letter of Interest

This Letter of Interest (LOI) pertains to Treasury Board of Canada Secretariat's (TBS) requirement for a single contractor to provide administrative claims processing services for the Public Service Health Care Plan (PSHCP) Administrative Services Only (ASO) requirement.

The purpose of this LOI is to:

a) inform industry of TBS's requirement for PSHCP ASO services;
b) seek feedback on industry best practices relating to claims processing administrative services;
c) share Canada's proposed procurement approach; and
d) invite industry to provide feedback, concerns and/or recommendations to Canada prior to finalizing the procurement approach and the Request for Proposals (RFP).

1.2 Nature of this Letter of Interest

This is not a bid solicitation. This LOI will not result in the award of any contract. Potential suppliers of any goods or services described in this LOI should not reserve stock or facilities, nor allocate resources, as a result of any information contained in this LOI. This LOI will not result in the creation of any source list. Therefore, whether or not a potential supplier responds to this LOI will not preclude that supplier from participating in any future procurements. Also, the procurement of any goods and services described in this LOI will not necessarily follow this LOI. This LOI is simply intended to solicit feedback from industry with respect to the subject matter described in this LOI.

2. INSTRUCTIONS FOR RESPONDING TO THIS LETTER OF INTEREST

2.1 Nature and Format of Responses Requested

Respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this LOI could be satisfied or improved. LOI responses should clearly identify any additional information and/or clarifications that respondents suggest to be incorporated into any future solicitation documents. Respondents are also invited to provide comments regarding the content, format and/or organization of any documents included in this LOI. Respondents should explain any assumptions made in their responses. Any marketing or promotional information submitted as part of the responses will not be reviewed and will not be considered in any future solicitation documents.

Responses will not be used for competitive or comparative evaluation purposes, and thus the response format is not as rigorously defined as would normally be for an RFP. However, for ease of use and in order for the greatest value to be gained from responses, Canada requests that respondents follow the structure outlined in section 2.6.

2.2 Response Costs

Canada will not reimburse any organization for expenses incurred in responding to this LOI.

2.3 Treatment of Responses

Use of Responses: Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify the procurement approach, as well as any documentation contained in this LOI. Canada will review all responses received by the LOI closing date. Canada may, at its discretion, review responses received after the LOI closing date.

Review Team: A review team composed of representatives of Canada will review the responses. Canada reserves the right to hire any independent consultant or to use any Government of Canada (GOC) resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

Confidentiality: Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the *Access to Information Act*.

2.4 Follow-up Activity

Canada may, at its discretion, contact any respondent to follow up with additional questions or to clarify any aspect of a response.

Canada does not contemplate conducting post LOI submission review meetings with respondents. However, should such a review be required, respondents will be contacted by the Contracting Authority to arrange a closed meeting, assuming the respondent is in agreement.

2.5 Contents of Letter of Interest

The information contained in this document remains a work in progress. Additional requirements may be added in any future bid solicitation that may be published by Canada. Existing requirements may be deleted or revised, based on responses received. Comments regarding any aspect of the documents are welcome. This LOI also contains specific questions addressed to industry.

2.6 Format of Responses

Cover Page: If the response includes multiple volumes, respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number and the full legal name of the respondent.

Title Page: The first page after the cover page should be the title page, which should contain the following information:

(i) the title of the respondent's response and the volume number;

(ii) the name and address of the respondent;

(iii) the name, address and telephone number of the respondent's contact;

(iv) the date; and

(v) the LOI number.

Number of Copies: Canada requests that respondents submit 1 copy of their response in unprotected (i.e. no password) PDF format by email, if the size of the document is less than 5MB, to:

michael.randall@tpsgc-pwgsc.gc.ca

Alternatively, for response documents that exceed 5MB in size, Canada requests that respondents save 3 copies of their response in PDF (2003 or later) onto four USB memory drives and contact the Contracting Authority identified in 2.7 for delivery instructions.

Responses to this LOI may be in either of Canada's official languages, English or French.

2.7 Enquiries

All enquiries and other communications related to this LOI and associated industry engagement activities shall be directed exclusively to the PWGSC Contracting Authority. Since this is not a bid solicitation, Canada will not necessarily respond to enquiries in writing or by circulating answers to all respondents; however, respondents with questions regarding this LOI may direct their enquiries to:

Contracting Authority:

Michael Randall
Public Works and Government Services Canada
Health Services Projects Division, Acquisitions Program
Services and Technology Acquisition Management Sector
Les Terrasses de la Chaudière, 10 Wellington Street, 5th Floor
Gatineau, Quebec, Canada
K1A 0S5

Telephone No.: (613) 558-1053
Email address: michael.randall@tpsgc-pwgsc.gc.ca.

2.8 Submission of Responses

Time and Place for Submission of Responses: Organizations interested in providing a response should deliver it to the Contracting Authority identified at Article 2.7 above by the time and date indicated on page 1 of this LOI document.

Responsibility for Timely Delivery: Each respondent is solely responsible for ensuring its response is delivered on time to the correct location.

Identification of Response: Each respondent should ensure that its name, return address, the solicitation number and the closing date appear legibly on the outside of the response.

Return of Response: Responses to this LOI will not be returned.

2.9 Public Service Health Care Plan Administrative Services Only Preliminary Procurement Timeline and Approach

Based on the results of this LOI process, Canada contemplates updating its requirements and publishing an initial Request for Information (RFI#1), which may include parts of a draft Statement of Work (SOW) for industry review and written feedback followed by subsequent one-on-one industry meetings. The one-on-one meetings will provide RFI#1 respondents an opportunity to meet with Canada's procurement team on an individual one-on-one basis to clarify their respective written responses.

Following the RFI#1 process, Canada contemplates publishing a second Request for Information (RFI#2) which will include a draft RFP, containing a near completed SOW and evaluation criteria for industry review and written feedback. Canada does not contemplate holding one-on-one meetings with industry as part of the RFI#2 process.

Feedback from the LOI and RFI processes will be taken into consideration by Canada when finalizing an RFP.

The following table provides a snapshot of the key procurement milestones and their associated target dates. Please note that these milestones, the associated target dates and all other information provided herein relating to the contemplated procurement approach are preliminary estimates which have been provided for general information purposes only. Canada reserves the sole right to delete, add or change any milestone, associated target date and any other aspect of the contemplated procurement approach as Canada deems appropriate.

PSHCP Administrative Services Only Requirement Target Procurement Milestones		**Target Date**
1	Publish Letter of Interest (LOI)	Winter 2018
2	Publish RFI #1 *(RFI#1 process to include one-on one meetings with industry post RFI#1 close.)*	Summer 2018
3	Publish RFI #2 *(RFI#2 to include a comprehensive draft RFP for industry review/feedback).*	Winter 2019
4	Publish Final RFP	TBD
5	Award Contract	TBD

3. FAIRNESS MONITOR SERVICES

Canada has engaged the services of an organization to act as an independent, third-party Fairness Monitor (FM) for the PSHCP ASO procurement process. The role of the Fairness Monitor is to provide an attestation of the fairness, openness, and transparency of all monitored activities of this procurement process.

The Fairness Monitor's duties will include, but will not be limited to the following:

i. observing all or part of the procurement process (including, but not limited to, the engagement process (LOI, RFI#1 including industry one-on-one meetings and RFI2) and the contemplated RFP process);

ii. providing feedback to Canada on any potential fairness issues; and

iii. attesting to the fairness, openness and transparency of the entire procurement process.

Please note that, for the purpose of carrying out its Fairness Monitor related obligations, the Fairness Monitor will be granted access to industry responses and related correspondence received by Canada pursuant to this LOI (any subsequent RFI(s) and any resulting RFP) and may act as an observer at any subsequent follow-up engagement and contracting activities.

PART II: BACKGROUND, AND OVERVIEW OF THE REQUIREMENT AND CONTRACT TERMS

4. BACKGROUND

The PSHCP provides voluntary, supplementary health care benefits to public service employees, employees of designated separate employers, MPs and senators, retired public service employees, and eligible dependents as well as dependents of the Canadian Forces and the Royal Canadian Mounted Police (RCMP). As of December 31, 2017, the PSHCP had over 669,000 members, of which almost 324,000 are retired members, and covers over 1.5 million members and their dependents. It is the largest employer-sponsored health care plan in Canada with total annual expenditures of approximately $1.22B.

The purpose of the PSHCP is to reimburse Plan participants for the reasonable and customary costs they have incurred for eligible services and products as described in the Plan Document after they have taken advantage of benefits provided by their provincial or territorial health insurance plan. The Plan also provides coverage to members who reside outside of Canada for basic health care services equivalent, as much as possible, to the services covered by provincial and territorial health care plans.

Detailed information about the PSHCP, including the plan document, eligibility information, appeals process, article and bulletins, etc. can be found at the following PSHCP websites:

http://www.pshcp.ca (*http://www.njc-cnm.gc.ca/directive/d9/en*)

5. OVERVIEW OF THE REQUIREMENT AND CONTRACT TERMS

5.1 PSPC will act as the designated procurement lead, on behalf of Treasury Board of Canada Secretariat, to acquire the services of a single contractor for the provision of health care claims processing and adjudication services for the PSHCP. The work under the contemplated PSHCP ASO contract, will include, but not be limited to:

1. **Claims Processing Services** - provides for the processing of various health benefits claims (e.g. electronic pharmacy benefit claims for prescription drugs, electronic and paper medical supplies and medical practitioner services, vision, hospital, emergency travel, and out of country claims). The claims processing services include, but are not limited to, claims adjudication, issuing payments for adjudicated claims and the preparation and distribution of claims statements. Members and Providers will have the ability to submit claims via the traditional mail methods, as well as digital services such as web, smartphone app and Provider E-services.

2. **Positive Enrolment Services** - this secure electronic and paper based solution service includes, but is not limited to, allowing members to positively enrol themselves and their eligible dependants, capture coordination of benefit information for themselves and their eligible dependants, collect consent for the use of their personal information, as well as

bank information (for claim reimbursement), email addresses (for electronic communications), and to allow for the preparation and delivery of the PSHCP benefit card, etc.;

3. **Communications and Information Services -** Communications and Information Services provide for ongoing communications with PSHCP members and providers through various methods such as, but no limited to, websites, online chat, call centres, and written communication products;

4. **Contract Management and Reporting Services** - Contract Management and Reporting services include, but are not limited to, the provision of:

   a) *Audit Services* to improve the integrity of the PSHCP (e.g., through the ability to detect PSHCP misuse and/or abuse, and claims processing errors). The goal of the Audit Services is to ensure claim payments and related financial transactions are correct and reflect PSHCP provisions, requirements and standards;

   b) A *Quality Assurance Program* to enable ongoing assessment and continuous improvement of business activities aligned with the PSHCP ASO contract work requirements (e.g. positive enrolment, electronic claims adjudication, provider communications, privacy requirements and security requirements, etc.);

   c) *Reporting Services* to support the ongoing management and reporting of the PSHCP (e.g. reducing risk, realizing efficiencies, enable understanding of plan activities and expenditures, and delivery of timely data, etc.). Reporting Services will be made available to the Project Authority and will include standard reports, an ad hoc reporting capability, dashboards, and annual reports including analysis and benchmarking;

   d) *Financial Management Services* – This service supports sound financial management practices for all aspects of the PSHCP. Guided by the *Financial Administration Act*, the service would be expected to deliver concise and accurate operational documents, business information, financial reports and respond to audit requirements on a timely basis; and

   e) *Business Management and System Maintenance Services,* which includes the development and provision of:

      i. Technical and Administrative Documentation (e.g. system manuals, security documentation, etc.);
      ii. System Management and Maintenance services;
      iii. Security;
      iv. Business Continuity and Disaster Recover Plans;
      v. Retention of Records;
      vi. Privacy (e.g. to ensure alignment with Government of Canada privacy legislation as well as *Personal Information Protection and Electronic Documents Act* (PIPEDA); and
      vii. Annual reviews of trends in the health benefit industry and associated recommendations for improving the administration of the PSHCP.

For additional information on the PSHCP, please refer to the most recent version of the PSHCP Directive (*http://www.njc-cnm.gc.ca/directive/d9/en*); including the Special Bulletins on Plan changes, http://www.pshcp.ca/news-and-bulletins/bulletins.aspx; and PSHCP Communiqués *http://www.njc-cnm.gc.ca/communique.php?id=38&lang=eng*.

5.2 Contract Period

The PSHCP ASO Contract Period will be defined following further internal and industry consultations. It is anticipated that Canada will issue a single contract for a period of eight years, with options to extend by one additional option period of two years plus two additional option periods of one year each, for a total of 12 consecutive years.

6. SECURITY REQUIREMENTS

6.1 There are no security requirements associated with this LOI.

6.2. Canada intends to have the following security clauses and the associated Security Requirements Checklist (SRCL) attached hereto under "*Annex A - Security Requirements*", form part of any contract resulting from the contemplated PSHCP Administrative Services Only RFP

a) The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) with Document Safeguarding at the level of **PROTECTED B**, issued by the Canadian Industrial Security Directorate (CISD), **Public Works and Government Services Canada (PWGSC**).

b) The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid **RELIABILITY STATUS**, granted or approved by the CISD/PWGSC.

c) The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of **PROTECTED B**.

d) Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.

e) The Contractor/Offeror must comply with the provisions of the:

i. Security Requirements Check List and security guide (if applicable), attached at Annex A;

ii. Industrial Security Manual (Latest Edition)

6.3 For information on personnel and organization security screening or security clauses, respondents are encouraged to refer to

i. the Industrial Security Program (ISP) of Public Works and Government Services Canada website http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html); and

ii. Public Works and Government Service Canada's (PWGSC) Canadian Industrial Security Directorate's (CISD) "*Contract Security Program roadmap for Government of Canada suppliers*" attached hereto under Annex A - Security Requirements.

6.4 With respect to the Contract Security Program Roadmap for Government of Canada Suppliers referenced in 6.3 ii. above and attached hereto under Annex A, please note that this document provides potential suppliers:

i. descriptions of the various types of Government sponsored security clearances;

ii. descriptions of the processes for industry to gain sponsorship and the associated estimated processing times to obtain such clearances; and

iii. other related security information.

6.5 For information purposes, respondents are hereby informed that the amount of time required to obtain the required security clearance levels may be lengthy and is contingent upon the specific clearance levels required. Bidders responding to any future PSHCP Administrative Services Only RFP will be solely responsible for obtaining such clearances. The contemplated PSHCP Administrative Services Only procurement will not be delayed to provide potential Bidders time to obtain required security clearances.

PART III: QUESTIONS TO INDUSTRY

Canada requests that LOI respondents provide written responses to each of the below questions. When responding, please ensure your answers are detailed and contain the rationale to support your suggested feedback.

7. COMMERCIAL QUESTIONS:

1) Proposed Procurement Timeline and Approach: Respondents are asked to provide feedback on the strengths, weaknesses and general feasibility of the PSHCP ASO procurement timeline and approach identified in 2.9 of this LOI *(initial LOI followed by RFI#1, RFI#2 and final RFP*) and provide any suggestions on how to make the process more efficient.

2) Security Requirements: Respondents are asked to provide comments on the contemplated PSHCP Administrative Services Only contract security clauses set out in article 6.2 of this LOI and the associated SRCL set out in the attached Annex A of the LOI. Please ensure that your response identifies, but is not limited to, any issues, concerns or recommendations with respect to the security requirements.

3) Contract Term and Option Periods: In accordance with article 5.2 of this LOI, Canada anticipates awarding a single PSHCP ASO contract for an initial period of eight years, with options to extend by one additional option period of two years plus two additional option periods of one year each, for a total of 12 consecutive years.

   Canada seeks your comments on the contemplated contract term and option periods. Please ensure that your response identifies whether the length of the anticipated contract term and option periods should be increased or decreased. If so indicate what would be optimal for both Canada and the selected contractor and provide the rationale to support your response.

4) PSPC plays an important role in helping the Government of Canada (GoC) achieve socio economic policy goals such as green procurement, innovation, job creation and the development of small and medium enterprises (SMEs). These policy goals are outlined in the Minister of Public Services and Procurement's 2015 mandate letter, which states:

> *Modernize procurement practices so that they are simpler, less administratively burdensome, deploy modern comptrollership, and include practices that support our economic policy goals, including green and social procurement."*

This includes:

> *"developing initiatives to increase the diversity of bidders on government contracts, in particular businesses owned or led by Canadians from underrepresented groups, such as women, Indigenous Peoples, persons with disabilities, and visible minorities, and take measures to increase the accessibility of the procurement system to such groups while working to increase the capacity of these groups to participate in the system.*

Question 4A

Please describe any initiatives the health care claims processing industry has implemented / or plans on implementing in the near future whereby government or non-government contract(s) were leveraged to address the above noted socioeconomic policy goals (*e.g. implantation of initiatives to increase the diversity of the health care claims processing industry workforce, in particular businesses owned or led by Canadians from underrepresented groups, such as women, Indigenous Peoples, persons with disabilities, and visible minorities; implementation of green procurement strategies; etc*.). Please ensure your response also includes examples of any such initiatives?

Question 4B

Canada is exploring the feasibility of leveraging the PSHCP ASO procurement to help address the above noted socioeconomic policy goals. Please provide feedback on how Canada might leverage the PSHCP ASO procurement to meet such goals? Please ensure that your response, includes but is not limited to:

- a list of the socioeconomic requirements (*e.g. implantation of initiatives to increase the diversity of the health care claims processing industry workforce, in particular businesses owned or led by Canadians from underrepresented groups, such as women, Indigenous Peoples, persons with disabilities, and visible minorities; implementation of green procurement strategies; etc*.) that could be addressed via the PSHCP ASO procurement;

- an associated description of how each socioeconomic requirement might be achieved; and

- your rationale to support your feedback.

Question 4C

Canada in exploring the feasibility of including specific socioeconomic bid evaluation requirements in the contemplated PSHCP ASO Request for Proposal (RFP) for bid evaluation purposes. Please provide feedback on the types socioeconomic bid evaluation requirements Canada might include in the contemplated PSHCP ASO RFP. Examples of such bid evaluation requirements are as follows:

a) The bidder certifies that a minimum of ___% of its resources preforming work under the contemplated PSHCP ASO contract will be from underrepresented groups such as women, Indigenous Peoples, persons with disabilities or visible minorities.

b) The bidder certifies that a minimum of ___% of the contemplated PSHCP ASO contractor's subcontract goods or services provided under the PSHCP ASO contract will be from a Diverse supplier/Social enterprise.

c) The bidder certifies that if awarded the PSHCP ASO contract, it will provide training to individuals from Diverse group(s) so that they can perform work under the resulting PSHCP ASO contract.

Diverse supplier is a business owned or led by Canadians from underrepresented groups, such as women, Indigenous Peoples, persons with disabilities and visible minorities. Each business is usually defined as being owned, operated and controlled by 51% of a given diverse group (e.g., women-owned business, Indigenous-owned business, persons with disabilities-owned business, or visible minority-owned business.

Social enterprises are another group of businesses that can help meet socio-economic objectives. A social enterprise seeks to achieve social, cultural or environmental aims through the sale of goods and services. The social enterprise can be for-profit or non-profit but the majority of net profits must be directed to a social objective (e.g., reducing environmental impacts of its products or including local training in communities) with limited distribution to shareholders and owners.

Diverse group includes representatives from a more specific social, cultural, or economic segment of the population such as Indigenous peoples, women, persons with disabilities, visible minorities, veterans, recent immigrants, LGBT, youth, unemployed, Socially/economically disadvantaged people.

8. TECHNICAL QUESTIONS:

Audits

1) Please describe the industry best practices for audits on medical practitioners who use provider digital services for claims submission (e.g. what is the typical frequency of such audits, what would trigger an audit, how are they conducted, who performs the audits, what information is audited, are audit results shared with the client, what are the typical deficiencies and how are they addressed, etc.)?

2) Please briefly describe the standard industry audit processes for electronic health (non-pharmacy) Providers? Generally, what percentage of industry e-claims for electronic paramedical Providers are submitted through Provider digital services vs. member website and smartphone app transmission methods?

3) Please describe typical industry standard audit and investigation protocols in cases where collusion between members and Providers is suspected? How would health care claims processing administrators typically pursue these investigations and make recoveries?

4) Please describe how a claims processing administrator's audit processes for emergency travel and out-of-country claims would typically be structured? Please describe the specific processes used to establish Reasonable & Customary amounts for out-of-country services and products. What are the industry best practices regarding conversational translation processes for out-of-country claims in foreign languages.

Call Centre

5) Would health care claims processing administrator's call centre systems typically allow for importing and exporting of call logs and recorded calls when required during either, implementation of a new contract, close out of an old contract or for the purposes of an audit or appeal?

6) With respect to a typical health care claims processing administrator, how would First Call (Contact) Resolutions (FCR) be measured and evaluated?

7) What are the typical current industry service level standards for out-of-country and emergency travel assistance call centres?

Claims Processing

8) Please describe how health care claims processing administrator's systems would typically handle Reasonable and Customary. Would Reasonable and Customary be hard-coded in their respective claims processing systems? Are there limits to the number of Reasonable and Customary codes that can be hard-coded into such systems?

9) Please describe how health care claims processing administrators would typically determine, maintain and update Reasonable and Customary limits. Through transition from an existing claims

processing administrator to a new claims processing administrator, how are differences in Reasonable and Customary charges typically handled. Please also clarify whether Reasonable and Customary limits are categorized by province or territory.

10) Please describe how health care claims processing administrators would typically make Reasonable and Customary limits available to plan members.

11) How would health care claims processing administrators typically allow for a client to have a customized formulary, with full drug cost components (e.g. mark-up, ingredient cost, dispensing fee and professional fee for each province/territory)?

12) Would health care claims processing administrators typically have an electronic solution to capture and maintain provider information and in turn use this information for the adjudication of claims (i.e. is the information used to confirm a legitimate provider before payment)? If so, please describe the electronic solutions which industry would typically employ?

13) With respect to health care claims processing administrators, if a client developed its own third party Provider agreements, would a claims processing supplier typically agree to facilitate the signing of such third party client Provider agreements and if so, would health care claims processing administrators have any concerns/caveats in doing so?

14) Please identify the current claims submission methods used by industry for the submission of drug and extended health claims? Please identify the known up and coming technological claim submission methods which industry will likely employ in the future? Please ensure your response also identifies:

    i) when industry believes each up and coming method will be adopted in the marketplace; and

    ii) the risks & benefits of employing each up and coming method.

15) Would typical health care claims processing administrators scan all paper claims, referrals and supporting documentation into their respective claims processing systems and if so, how long would they retain paper copies?

16) If health care claims processing administrators do scan paper claims into their respective claims processing systems, please describe the process used when a claim comes in for a referral. Would referrals be scanned separately or would the referral be attached to the first scanned claim?

17) Do health care claims processing administrators use questionnaires (completed by Medical Doctors) to gather medical information? If so, what expenses are questionnaires used for? If not, how would industry gather information required to process claims that require additional information?

18) Under the contemplated Public Service Health Care Plan Administrative Services Only contract, should Canada expect cost savings (i.e. different rates charged to Canada) for the adjudication of

paper claims versus claims paid using drug/benefit card versus e-claims/mobile? If so, what would the approximate difference (%) be between all methods?

19) Should the Public Service Health Care Plan claims processing requirement be awarded to a new contractor (i.e. not the incumbent) under the contemplated procurement process, could Public Service Health Care Plan Members maintain their current Public Service Health Care Plan policy Number and Certificate Number under the new contract?

20) For drug and health benefits, please provide a list and associated short description of the types of edits (hard and soft), by benefit type, available on typical industry claims processing systems?

21) From an industry perspective, are expenses (i.e. prescription eye glasses, medical supplies/devices) purchased outside of Canada (physically or online) eligible for electronic claim submission (e.g. web claims, smartphone app, etc.)?

22) For all Coordination of Benefit claims, would health care claims processing administrators typically differentiate between Internal (same plan) and external (different plan under same company and plan with another Administrator) Coordination of Benefits? Is this breakdown captured during claims processing? If yes, can this be reported on through a reporting solution?

23) Would health care claims processing administrators typically fully integrate with Ontario Drug Benefit deductible and other provincial-territorial plans? For provincial-territorial plans that have a deductible, would health care claims processing administrators typically capture and report on the amount of the deductible applied and outstanding?

24) Would health care claims processing administrators typically offer Provider digital services (paramedical practitioners, ophthalmologist, and optometrist) and the associated capability for Providers to allow for electronic claims submission and payment to the Provider directly (members pay out-of-pocket portion)? If so, would health care claims processing administrators have the capability to process Coordination of Benefits with another member that is a part of the same plan (internal coordination of benefits)?

25) For Medical Supplies and Equipment, would health care claims processing administrators typically create pseudo-DINs for these items or would they place them under a category in their claims processing and reporting systems?

26) Please describe how a health care claims processing administrator would typically capture and report on claim drug cost components? What drug cost components can administrators capture and report in each province/territory?

27) With respect to typical health care claims processing administrators, how are claims adjustments (i.e. refunds, overpayments, corrections, reissued stale-dated cheques) processed and reported in claims transactional data? How is historical reporting reconciled once adjustments are made?

28) Please describe industry best practices for adjudicating out-of-country claims, particularly in regard to the application of pricing schedules or Reasonable and Customary amounts?

29) How would a health care claims processing administrator typically ensure that prescribed products and services are "medically necessary" and whom would make this determination?

30) How would a health care claims processing administrator's Drug Utilization Review process work? How would outlier claim submissions be identified and what processes would be used to follow through on these cases?

31) Please describe how health care claims processing administrators for out-of-country claims would report on negotiated discounts and associated fees at a detailed claims level?

32) From an industry perspective, for all electronic claims submission methods is the functionality available to submit images, including a referral, on first submission of a claim without a claim rejection?

33) Please describe the typical current industry service level standards for out-of-country and emergency travel assistance claims processing.

Communications

34) Please identify current industry communication methods used by health care claims processing administrators to reach out to members and vice versa (e.g. live chat, secure messaging). Please identify the known up and coming technological methods which industry will likely employ in the future? Please ensure your response also identifies:

    i) when industry believes each up and coming method will be adopted in the marketplace; and

    ii) the risks and benefits of employing each up and coming method.

35) Please describe the methods/how a health care claims processing administrator would conduct regular communications with a membership of approximately 650,000 in a cost-effective manner?

Data Migration

36) How would a health care claims processing administrator typically securely transfer claims history and member information/positive enrolment data to a new Administrator? Please describe the process, the associated timing for doing so, risks & risk mitigation strategies employed, caveats, etc.

37) When transitioning from an incumbent health care claims processing administrator to a new health care claims processing administrator, how long would it typically take for the new health care claims processing administrator to:

i) Assess the quality/accuracy of the incumbent's source data; and
ii) Migrate, convert and load such data into its claims processing system?

With respect to the above, the incumbent data would include claims history and all supporting data such as provider, member, dependant, drug pricing tables, etc.

Eligibility

38) Is it industry best practice for a health care claims processing administrator to confirm full time student's status on an annual basis for all over age dependants? (i.e. requiring members to provide proof that their over age child continues to attend a post-secondary institution on a full time basis). If yes, would a health care claims processing administrator typically allow for members to submit proof electronically via member website and/or smartphone app? Also, what is the timeframe that members have (i.e. September to December) to provide such proof on an annual basis and would a health care claims processing administrator's member website and smartphone app allow for pop-up reminders to be given to members upon log-in?

Finance

39) Please describe the types of banking arrangements health care claims processing administrators currently have for claims processing. For example, bank account with line of credit arrangement; Zero-balance account, etc.

40) With respect to the response to question 39, please describe industry's typical bank reconciliation process(es) for each type of bank account, and provide sample supporting reports (or descriptions of the reports) pertinent to the process.

41) Please describe industry's typical process for the management of stale-dated cheques issued to members.

42) Please provide a description of a billing process employed by a typical industry health care claims processing administrator to bill its clients. Please ensure that your response includes, but is not limited to, a brief description of the typical:

(i) billing cycle frequency (e.g. monthly, quarterly, etc.);
(ii) work components billed under a typical invoice; and
(iii) the types of credits and recoveries which may, where applicable, be applied to a typical invoice?

*As part of your response, please also provide sample reports (or a description of the types of data included in a typical report) that an in*dustry health care claims processing administrator would provide to its client and the associated frequency *such reports would be provided?*

43) With respect to typical health care claims processing administrators, please provide brief descriptions of industry practices/methods used for the recovery and tracking of overpayments

from members and/or service provider partners for reasons that may include, but are not limited to, administrative errors, legal judgements, audits, etc. Please ensure that your response also includes a list of recovery methods used by type, and where available please also provide sample reports illustrating how such recoveries are reported to a client.

44) Please describe how a typical health claims processing administrator would validate the accuracy of its reports prior to submitting such reports to a client for acceptance? Would such reports be reviewed and validated by a CPA prior to being submitted to a client for acceptance?

Member and Provider Websites

45) How would health care claims processing administrators indicate to plan members or Providers that new information (e.g. Member Newsletter, plan change, website changes, claim status update, etc.) is available, while they are viewing a website or smartphone app?

Provider Agreements and Registration

46) Is it industry best practice to have separate provider agreements for pharmacies, medical practitioners and hospitals? If yes, why and how do these differ?

47) How are hospital Providers typically treated in regard to registration services (i.e. are they registered to direct bill)? Can hospital Providers use Provider digital services?

Quality Assurance

48) Under the contemplated Request for Proposal (RFP), if Bidders are required to submit a Quality Assurance plan as part of their respective Bids, what supporting / background information would Canada need to include in its RFP for Bidders to develop a comprehensive proposed plan?

Reporting Solutions

49) Would health care claims processing administrators typically provide an ad hoc reporting system that allows for the querying of all plan data, including historical data and downloading of large data files? If yes, please describe how health care claims processing administrators would capture and organize claims and supporting data? Would all data be available in detailed and summarized formats? Would the data structure be customized for each client to capture their needs?

50) Would health care claims processing administrators typically have the ability to provide customizable management dashboards based on claims information and select data fields?

51) How do health care claims processing administrators typically achieve data integrity, including balancing across reports and internal consistency? What validation processes are typically in place?

Security

52) What is industry standard practice for issuing passwords to register for online services? What authentication controls are included in such processes?

Sub-Contractor Compliance

53) Please describe how health care claims processing administrators would ensure sub-contractor compliance with a plan sponsor's contract? Would a health care claims processing administrator receive regular reporting or meet with sub-contractors regularly to discuss performance and compliance?

Systems

54) Would a health care claims processing administrator's claims processing system typically have the ability to change business rules without requiring system modifications (i.e. flexible coding technology) which would allow for more cost-effective implementation of on-going policy and program changes?

Glossary

Drug Utilization Review - an authorized, structured, ongoing review of prescribing, dispensing and use of medication. Drug Utilization Review encompasses a drug review against predetermined criteria that results in changes to drug therapy when these criteria are not met.

Emergency Benefit While Travelling – benefit for eligible medical expenses incurred as a result of an emergency while travelling on vacation or on business.

> *Eligible expenses mean the reasonable and customary charges in excess of the amount payable by a provincial/territorial health insurance plan, if they are required for emergency treatment of an injury or disease which occurs within 40 days from the date of departure from the province/territory of residence.

Emergency Travel Assistance - The PSHCP provides a toll free number which gives participants 24 hour access to a world-wide assistance network. The network will provide:

1. transportation arrangements to the nearest hospital that provides the appropriate care or back to Canada;
2. medical referrals, consultation and monitoring;
3. legal referrals;
4. a telephone interpretation service;
5. a message service for family and business associates; messages will be held for up to 15 days;
6. advance payment on behalf of the participant or a covered dependant for the payment of hospital and medical expenses

First Call (Contact) Resolution – correctly addressing the customer's need the first time they call, thereby eliminating the need for the customer to follow up with a second call.

Reasonable and Customary - means that amount which is usually charged to a person without coverage and which does not exceed the general level of charges for the specific service or product in the geographic location where the expense is incurred, as determined by the Administrator. Published fee guides of national, provincial or territorial associations of practitioners will be consulted for this purpose where applicable.

Annex A - Security Requirements

This Annex A, includes the following:

i. Security Requirements Checklist (SRCL) for the contemplated PSHCP Administrative Services Only contract; and

ii. CISD's Contract Security Program Roadmap for Government of Canada Suppliers

JAN 0 4 2017

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
24062-180558
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: Treasury Board Secretariat of Canada
2. Branch or Directorate / Direction générale ou Direction: Pensions and Benefits
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
For the provision of a single competitively tendered contractor to provide Administrative Services Only Health Care Claims processing and adjudication services for the Public Service Health Care Plan.

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

6. Indicate the type of access required / Indiquer le type d'accès requis: Protected B Level - Personal Benefit Plan Coverage Information

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

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

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☑	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ☐	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
24062-180558

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?
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 :
TA ☑ No Non ☐ Yes Oui

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?
TA ☑ No Non ☐ Yes 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?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
TA ☑ No Non ☐ Yes Oui

If Yes, will unscreened personnel be escorted?
Dans l'affirmative, le personnel en question sera-t-il escorté?
☑ No Non ☐ Yes Oui

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS See Attached Contract Security Requirements.

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

11. b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?
TA ☑ No Non ☐ Yes 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?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?
TA ☑ No Non ☐ Yes Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)
See Attached Contract Security Requirements.

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?
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?
☐ No Non ☑ Yes Oui TA

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
24062-180558

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		✓														
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).

Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Better government: with partners, for Canadians

Contract Security Requirements - Protected B

Canada

1. INTRODUCTION

This document outlines the IT Security requirements that the Contractor must meet prior to the processing of sensitive data up to and including the level of *Protected B*. 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 by the Contractor in order that the processing of sensitive information be approved by the Public Works and Government Services Canada's 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. MANDATORY PREREQUISITES

2.1 PWGSC Validation for Physical Security

The application of the security safeguards listed in this document is based on the *mandatory requirement* that the physical premises have been inspected by the CISD, PWGSC. The Departmental Security Officer's (DSO) office will validate the certification and notify the IT Security Coordinator.

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*".

All Contractor personnel handling Government of Canada sensitive information must attend a training/briefing session coordinated and delivered by the Treasury Board Secretariat DSO, IT Security Coordinator.

2.3 Authorization and Access Control

The Contractor must provide the Treasury Board Secretariat IT Security Coordinator with a list of all individuals who have access to the sensitive information being processed for the Department, along with Contractor current policies and procedures for adding individuals to the environment and the process followed when an individual is removed from the environment.

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

2.4 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 Treasury Board Secretariat. 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*". Contractor personnel may only transport documents associated with this Contract into or out of the WPS Protected B physical domain with the approval of the Treasury Board Secretariat's DSO.

2.5 Security Policy Compliance Monitoring

On a frequency to be determined by the Departmental Security Officer or the IT Security Coordinator, the Treasury Board of Canada Secretariat 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 sensitive information.

3. MINIMUM SECURITY REQUIREMENTS (DETAILS)

3.1 Physical Security

Company must provide and/or demonstrate proof of:

- Brief description of the organization's role and facility
- Signed Company Security Orders
- Material control log for Protected information and assets
- Visitor control log for Protected information and assets
- Detailed signed floor plan identifying the reception zone and the operation zone; plan must include all entries (doors and windows) and the location of all equipment being used to produce, store, destroy and/or transmit data
- Pictures of zones, doors, windows, cabinet, shredder and IT equipment
- RCMP approved containers for storing information at the protected A and B levels
- RCMP approved destruction equipment, or the name of a shredding company that is cleared to the appropriate level
- An appropriately security cleared cleaning organization, or cleaning done under supervision during regular working hours

3.2 Personnel Security

- All individuals must hold a valid reliability status or higher
- The maintenance of this status is required for the duration of the contract

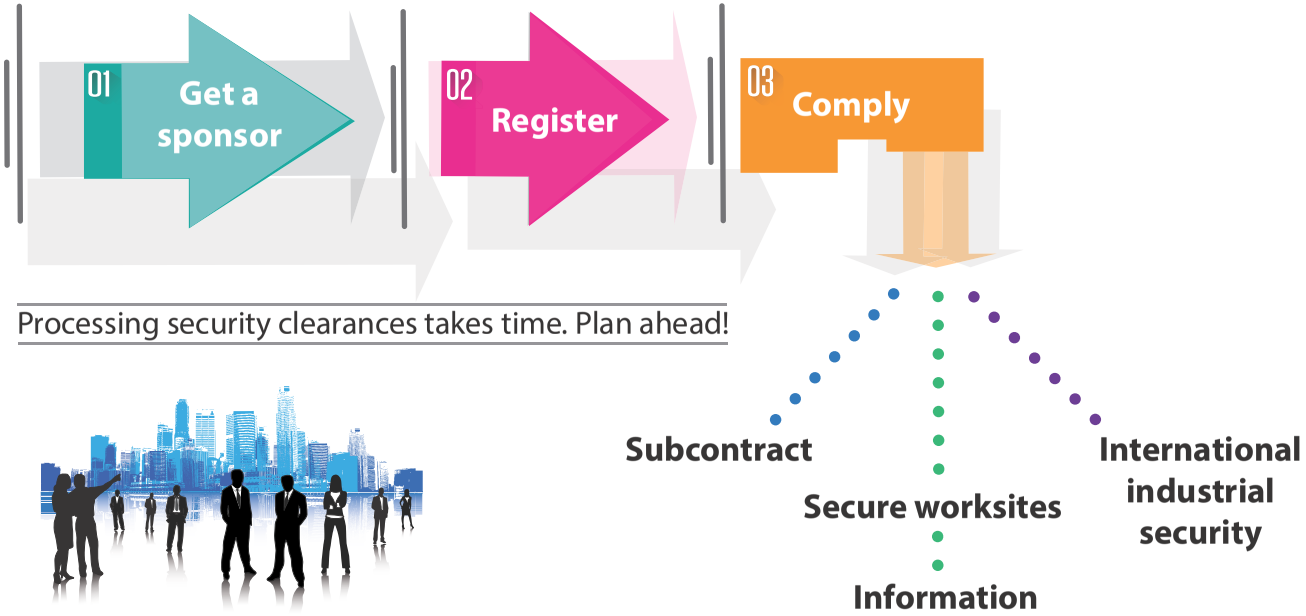
3.3 IT Security

- Any loss or theft of PROTECTED information must be reported by the Contractor to the Project Authority within 2 hours of detection.
- Any computers used to store and/or process PROTECTED information shall be located in a space that meets the requirements of an Operations Zone as defined in the Treasury Board's Operational Security Standard on Physical Security.
- If PROTECTED information is stored or processed on portable storage devices such as USB flash drives, the information must be protected by a strong password and encrypted using a product that meets Government of Canada (GC) encryption standards as defined in ITSA-11E CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within GC.
- When sending PROTECTED B information electronically via email or other electronic exchange, it must be protected by a strong password and encrypted using a product or service that meets GC encryption standards as defined in ITSA-11E CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within GC.
- All PROTECTED information in the Contractor's custody shall be stored on physical computers and storage media in their custody and located in Canada only. The use of third-party cloud services (e.g. Google Drive, Dropbox) to store PROTECTED information is prohibited.
- On all computers used to store and/or process PROTECTED information:
    - Current antivirus software must be installed and maintained with the most current virus definitions and signatures;
    - Operating System (OS) must be a vendor-supported OS (i.e. current security patches must still be available and the product not have reached end of life) and the most recent OS and application security patches must be installed and updated with the most current version;
    - Access to the information must be restricted by requiring a unique user account ID and strong password for each user who will access the information or use the computer on which it sits;
    - Computer accounts must not be shared.
    - A password protected screen saver set to 15 minutes or less must be enabled; and,
- All computers used to store and/or process PROTECTED information, which are also connected to the Internet, should reside behind a network router that is securely-configured using industry best practices (e.g. NAT-enabled firewall, password-protected and documented configuration, security logging enabled, maintained and reviewed, filtered access).
- Security event logging must be enabled and logs kept for a minimum of 90 days.
- If there is a requirement to service a computer that is used to store and/or process PROTECTED information outside of the Contractor's premises, any hard disk(s) containing PROTECTED information must be removed and secured with the Contractor prior to the computer being removed from the premises.
- If it has been determined that a computer hard disk used to store and/or process PROTECTED information is no longer serviceable, the hard disk must be surrendered to the Project Authority for destruction.

- When devices such as a computer hard drives, portable hard drives, USB storage drives and any other devices used to store/process PROTECTED information are no longer required to store/process the information, the information must be securely deleted and the remaining free space on the device securely wiped, in accordance with industry best practices
- When PROTECTED information is being displayed on a computer screen or being viewed in printed format, it must not be viewable by unauthorized persons.
- If remote access to the contractor's Information System (i.e. computers & storage devices) and the PROTECTED information contained therein is required, the remote access configuration must be securely-configured using industry best practices (e.g. encrypted connection, two-factor authentication, security logging, no split tunneling, access control lists, remote access software provided by Contractor to employee).
    - Any employees using the remote access must also meet all requirements listed in this document with regards to their remote location and equipment used there.

Public Services and Procurement Canada | Services publics et Approvisionnement Canada

Contract Security Program roadmap for Government of Canada suppliers



Contact us:

National Capital Region: 613-948-4176
Toll-free: 1-866-368-4646
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src/

Consult the main roadmap

Public Services and Procurement Canada | Services publics et Approvisionnement Canada

Note: Subject to change based on program updates.

Contract Security Program roadmap for Government of Canada suppliers

Get a sponsor

Learn + Find + Apply

01

An organization must be sponsored by a Government of Canada (GC)-approved source to register with Public Services and Procurement Canada (PSPC).

A GC-approved source must submit a request for Private Sector Organization Screening (PSOS) to PSPC.

In the PSOS the GC-approved source must clearly demonstrate that an organization will need access to sensitive information, assets or worksites as part of a government contract or subcontract with security requirements.

Canadian prime contractors who wish to subcontract to an organization that is not registered with the PSPC Contract Security Program (CSP) can sponsor the subcontractor and must complete and submit a security requirements checklist (SRCL) (TBS/SCT 350-103) along with the PSOS.

Note: Canadian prime contractors who wish to sponsor, must also be in good standing with the CSP and have an active GC contract.

Register

If sponsorship is approved, the PSPC will contact the organization directly to initiate the registration process.

The PSPC will send a registration package containing a series of forms to the organization for completion.

02

Appoint a security official

To register with PSPC an organization must appoint a company security officer (CSO) and one or more alternate company security officers (ACSO).

CSO responsibilities

CSOs are accountable to the PSPC on all contract security matters.

Types of organization clearances:

Designated organization screening (DOS)

Protected A, B, C information/assets

Timeline to acquire: **up to 6 months**

Facility security clearance (FSC)

Secret, top secret information and assets

Timeline to acquire: **6 months or more**

Comply

Security of information and assets

Organizations are responsible to ensure the protection of government sensitive information and assets entrusted to them.

This includes when: transferring or exchanging sensitive government of Canada information or assets in Canada or abroad.

03

Screen your personnel

A personnel security screening is required for employees who need to access federal government protected or classified information, assets and work sites as part of a contract.

Personnel security clearances

Reliability status & Secret clearances are valid for **10 years.**

Top Secret is valid for **5 years**.

An employee can only start to work on a contract when granted a security clearance and briefed on related security responsibilities.

Maintain your organization security clearance

The information that the organization supplies to obtain its clearance must be kept up to date and any changes to this information must be reported to the PSPC as soon as it changes.

Other security requirements

Subcontract

Responsibility A prime contractor is responsible to get approval from PSPC before subcontracting work.

Sponsor The prime contractor must complete a security requirements checklist (SRCL) and submit it with a request for private sector organization screening (PSOS) form to PSPC to sponsor a subcontractor into the program.

Screen Subcontractor The subcontractor's organization and personnel must be cleared before work can begin.

Secure worksites

Document safeguarding capability (DSC)
If an organization is required to store sensitive GC information and assets, physically and/or electronically at their worksites, they need to obtain document safeguarding capability through PSPC.

To obtain DSC, an organization must first obtain a valid **DOS** or **FSC.**

Information technology security (IT)
The authority to produce, process and store protected or classified GC information is also subject to PSPC approval.

International industrial security

Canada negotiates bilateral security instruments with various countries.

List of countries with bilateral security instruments.

Request for visits Contact PSPC for approved to visit a secure government and/or organization site in Canada or abroad.

Foreign contracts Contact PSPC to learn more about international contracts.

Contact us:

National Capital Region: 613-948-4176
Toll-free: 1-866-368-4646
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src

Also see our individual reference sheets:
www.tpsgc-pwgsc.gc.ca/esc-src/ressources-resources-eng.html

Public Services and Procurement Canada | Services publics et Approvisionnement Canada

Note: Subject to change based on program updates.

Contract Security Program

Get a sponsor

Reference sheet

Approved sources

A private sector organization must be sponsored by a Government of Canada (GC) approved source to register in the Public Services and Procurement Canada (PSPC) Contract Security Program (CSP).

GC-approved sources

- federal government: procurement officers, security officers, project officers
- private sector organizations (also referred to as "prime contractors"), who are registered in the PSPC program, are in good standing and who hold an active GC sensitive contract (for subcontracts they require to subcontract on)
- foreign national or designated security authorities (NSA/DSA), or the PSPC

The approved Canadian source must submit a request for private sector organization screening (PSOS) form to PSPC along with a security requirements checklist (SRCL) for subcontracts.

www.tpsgc-pwgsc.gc.ca/esc-src/organisation-organization/enquete-screening-eng.html#s3

30% Complete

Contact us:

Toll-free: 1-866-368-4646
National Capital Region: 613-948-4176
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src

Sponsorship process

In the PSOS, the approved source **must clearly demonstrate** that an organization will need access to sensitive information, assets or worksites as part of a government contract or subcontract with security requirements.

PSPC will contact the sponsored private sector organization in order to collect the necessary information to appoint and security clear a company security officer (CSO), and key senior officials (KSO) as required.

Sponsor a subcontractor

Canadian prime contractors who hold an active contract and are in good standing with the PSPC program must submit a private sector organization screening (PSOS) form for a **subcontractor** who is not registered with the PSPC CSP.

The Canadian prime contractor must also complete and submit a security requirements checklist (SRCL) (TBS/SCT 350-103) that identifies the subcontract security requirements to PSPC.

60% Complete

Sponsorship process cont'd

If document safeguarding is required PSPC will appoint a **field industrial security officer** (FISO) to schedule and conduct a physical security inspection of the organization's facility.

PSPC will conduct the necessary security screenings for the newly appointed company security officer (CSO) and key senior officials (KSO)s, as required.

PSPC will then send an email to the organization to initiate the organization security screenings.

The organization must then return all duly completed forms within **30 days** of receipt, to PSPC.

PSPC will advise the organization if the organization security clearance has been granted. If granted, PSPC will send the briefing certificate and the CSO or alternate company security officer (ACSO)

If the approved source failed to demonstrate the contractual requirements, they'll be advised that their sponsorship was rejected and why.

100% Complete

Next step: register

Contract Security Program

Register

Reference sheet

Register

Once an organization receives their registration package, they have **30 days** to complete and submit the registration forms to the Public Services and Procurement Canada (PSPC) Contract Security Program (CSP).

Registration forms

- Application for registration provided by CSP
- Corporate company security officer/ company security officer security appointment and acknowledgement and undertaking (Annex 1-A)
  Alternate company security officer ACSO
- Appointment and acknowledgment form (Annex 1-B) (if applicable)

- Personnel screening, consent and authorization form
  - (TBS/SCT 330-23) used to request reliability status screening for the Company Security Officer (CSO)
- Security Clearance form
  - TBS 330-60 used to request Secret and/or Top Secret screenings for the CSO and key senior officials (KSO)s

Note: The 330-60 must always be accompanied by a completed (TBS 330-23).

- Public Services and Procurement Canada-Security agreement (Annex 3-G)

Note: Additional documents may be required.

If an organization needs document safeguarding capability (DSC), please consult our secure worksites reference sheet.

60%
Complete

Contact us:

Toll-free: 1-866-368-4646
National Capital Region: 613-948-4176
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src

Appoint a security official

During the PSPC CSP registration process, the organization will need to appoint a company security officer (CSO) and an alternate company security officer (ACSO).

PSPC is not authorized to provide information on private sector organizations or personnel registered in the CSP except to the CSO or ACSO.

A company security officer must be:

- an employee of the organization
- physically located in Canada
- a Canadian citizen or permanent resident of Canada
- security screened at the same level as the organization

Processing times for personnel security screening requests

Reliability status (simple): 7 business days
Reliability status (complex)**:** 120 business days
Classified security clearance: 75 business days (in addition to reliability screening timelines)

There is no cost to register with the PSPC CSP.

100%
Complete

CSO responsibilities

Organization security

- appoint, brief and train ACSOs
- inform the CSP of any changes in key senior officials (KSO)s
- inform the CSP about organizational changes (new address, new KSO, etc.)
- report
  - changes in employee's behaviour
  - changes in circumstances
- termination of employment (must give formal debriefing)

Personnel security

- apply for security screening for personnel
- brief employees (security briefing)
- maintain a list of all cleared personnel
- upgrade clearances when required

Validity of personnel security screenings

Reliability status: valid for 10 years
Security clearance: (**Secret**) - valid for 10 years (**Top Secret**) - valid for 5 years

Processing times for organization clearance requests

Designated organization screening (DOS)
Protected A, B or C information and assets:
up to 6 months

Facility security clearance (FSC)
Secret or top secret information and assets:
6 months or more

Next step: comply

Public Services and Procurement Canada | Services publics et Approvisionnement Canada

Note: Subject to change based on program updates.

Contract Security Program

Comply

Reference sheet

Security of information and assets

Transfer information and assets

Public Services and Procurement Canada (PSPC) ensures that information and assets that are transferred or exchanged as part of a sensitive Government of Canada (GC) contract, whether in Canada or abroad, are safeguarded throughout the process.

Aftercare

Aftercare comprises of a formal planned security briefing to personnel and the reporting of changes in circumstances, unusual incidents and behaviours.

Do not hesitate to report any suspicious behaviour, circumstances, or incidents by sending an email to:

ssidivisiondesenquetes.issinvestigationsdivision@tpsgc-pwgsc.gc.ca

Termination of employment

Upon termination of employment, engagement or assignment, all individuals must receive a formal debriefing. The security screening certificate and briefing form (TBS/SCT 330-47) is used to record that termination procedures have been completed.

Need-to-know principle

The need-to-know principle restricts employee's access to sensitive information and assets based only on their duties.

Access is not based on title, status, rank or level of clearance.

Contact us:

Toll-free: 1-866-368-4646
National Capital Region: 613-948-4176
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src

Screen your personnel

Log into the online industrial security services (OLISS) portal to fill out and e-sign all personnel screening forms.

Reliability status: Protected A, B, or C information, assets or work sites - (simple) **7 business days** - (complex) **120 business days**

Complete the form:
Personnel screening, consent and authorization form (TBS/SCT 330-23E)

Security clearance: Confidential, Secret, Top Secret, North Atlantic Treaty Organization (NATO) information, assets or worksites.

Classified security clearance request **75 business days**

Complete the forms:
Personnel screening, consent and authorization form (TBS/SCT 330-23E)
Security clearance form (TBS/SCT 330-60E)

Process times are based on complete and accurate forms.

Transfers and duplicates

If an employee already holds a screening with another government department or private sector company you can simply **transfer** that screening to your organization.

A clearance may be **duplicated** when the employee holds a valid clearance with one or more private sector organizations registered in the PSPC Contract Security Program (CSP).

Please note that **fingerprints** and **credit checks** are required for all new, update and upgrade personnel screening applications.

Maintain your organization security clearance

Organizations must report any corporate changes as soon as they occur to PSPC.

Upgrade organization clearance

To upgrade an organization clearance to a higher level clearance, a GC-approved source must sponsor the organization.

Abide by your security agreement form (annex 3-G)

The Public Services and Procurement Canada security agreement contains the terms and conditions that the organization agreed to comply with at all times during the contract.

Appointing an alternate company security officer

At least one alternate company security officer (ACSO) must be appointed at the facility of the organization where the company security officer (CSO) is located.

At least 2 security officers must be appointed at each additional facility of the organization with document safeguarding capability (DSC).

Appointing a new company security officer

Prior to departure, a CSO must ensure a new CSO is cleared, appointed and trained.

Go to:
- Subcontract
- Secure worksites
- International industrial security

Note: Subject to change based on program updates.

Contract Security Program

Subcontract

Reference sheet

Responsibility of the prime contractor

The prime contractor is the organization that wins the bid to work on a Government of Canada (GC) or a foreign government contract.

The subcontractor is hired by the prime contractor to work on part of a Canadian or foreign government contract.
A subcontractor is not an employee of the prime contractor.

The prime contractor is responsible to get approval from Public Services and Procurement Canada (PSPC) before awarding a subcontract with security requirements and delegating work.

A Canadian prime contractor, wishing to subcontract part of the work, who has an active GC-sensitive contract, standing offer or supply arrangement and is in good standing with the PSPC must:

1. sponsor the subcontractor by submitting the security requirements checklist (SRCL) and a private sector organization screening (PSOS) to PSPC
2. inform the subcontractor of their responsibilities
3. ensure each subcontract has a unique subcontract number

Remember that the subcontract cannot be awarded and work cannot begin until the subcontract is approved by PSPC.

Contact us:

Toll-free: 1-866-368-4646
National Capital Region: 613-948-4176
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src

Sponsor

When PSPC receives the subcontractor sponsorship request, they will review the request and:

1. verify if the subcontractor is registered
2. advise the prime contractor that work can or cannot begin

The subcontractor cannot begin work until their organization clearance has been granted and the subcontract approved by PSPC.

3. sign the SRCL, and provide security clauses

The subcontract may **not** necessarily have the same security clauses as the prime contract.

The prime contractor will then:

4. input the signed SRCL and security clauses into the subcontract
5. submit a copy of the subcontract, SRCL and security clauses (including any amendments to the subcontract) to PSPC

The process must be adhered to by all contractors wishing to subcontract work, including subcontractors allocating work to another subcontractor.

Screen subcontractor

Once the subcontracted organization receives their registration package, they will have **30 days** to complete and submit all registration forms.

If required, PSPC will also initiate a document safeguarding capability (DSC) inspection process.

Once PSPC has approved the subcontract, the subcontractor's company security officer (CSO) must obtain security screenings for all personnel who will be working on the subcontract and who will have access to the sensitive GC information, assets and worksite.

Processing times for personnel security screening requests

Reliability status (simple): 7 business days
Reliability status (complex) 120 business days
Classified security clearance: 75 business days (in addition to reliability screening timelines)

Before you enter into a subcontract with a foreign organization or get a classified contract from a foreign organization, your organization must contact PSPC. Click the link to read more about international subcontracting.

Return to the Contract Security Program roadmap

Note: Subject to change based on program updates.

Contract Security Program

Secure worksites

Reference sheet

Document safeguarding

When your organization is required to store sensitive Government of Canada (GC) information and assets, it needs to obtain a **document safeguarding capability (DSC)** through the Public Services and Procurement Canada (PSPC) Contract Security Program (CSP).

Before an organization can obtain a DSC, it requires 1 of the following 2 clearances (valid):

- Designated Organization Screening **(DOS)**
- Facility Security Clearance **(FSC)**

Note: A DSC clearance level cannot exceed that of the organization clearance.

DSC is site-specific and may result in a physical inspection by a field industrial security officer (FISO).

There is no cost for inspections, but organizations must pay for the cost of any equipment or construction required to safeguard information and assets at their worksite as per the CSP and contract security requirements.

Organizations are required to develop **security orders** with the assistance of the FISO. They must be submitted to the FISO appointed to their organization.

Contact us:

Toll-free: 1-866-368-4646
National Capital Region: 613-948-4176
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src

Document safeguarding subsets

Information technology

The authority to produce, process and store protected or classified information electronically is subject to PSPC approval.

Consult the information technology security reference sheet for further details.

For organizations with DSC, a minimum of 2 security officers, cleared to the level of DSC are required at each of the secure work sites.

Production

Production is a broad term that can encompass organizations required to build, manufacture, repair, retrofit or reproduce sensitive material or products at its site or sites.

COMSEC

COMSEC stands for Communications Security. COMSEC material is designed to secure or authenticate telecommunications information.

The Communications Security Establishment is Canada's national COMSEC authority and is involved in granting COMSEC clearances.

IT security, production and COMSEC are contract specific and only valid for the duration of the contract.

Inspection process

Before the inspection

A FISO with PSPC will review the following documents:

- security requirements checklist (SRCL) form
- request for private sector organization screening (PSOS) form
- contract security clauses
- statement of work

During the inspection

The FISO will identify:

- potential targets or risks for physical attacks
- intrusion detection systems
- physical security zones in accordance with the federal Operational Security Standard on Physical Security
- how information and assets are handled

The FISO will take or request photographs of:

- all interior and exterior access points, including locking hardware
- storage cabinets and their location
- access control doors to operations or security zone (if applicable)
- server room(s)

After the inspection

The organization can begin work on the contract once the inspection process is complete **and** the organization has been notified by PSPC in writing that they possess the required security level.

Inspections may be conducted at any time throughout the life of the contract.

Inspection timeframes will vary based on security levels and an organization's ability to comply with PSPC's recommendations.

Next step: information technology

Public Services and Procurement Canada | Services publics et Approvisionnement Canada

Note: Subject to change based on program updates.

Contract Security Program

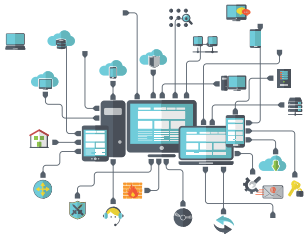
Information technology security

Reference sheet

Authority to process

To obtain the authority to process information technology (IT) designation, organizations must hold a valid:

- Designated organization screening (DOS) or a Facility security clearance (FSC)
- Document safeguarding capability (DSC)



Your organization will need to:

- ensure their company security officer (CSO) understands IT requirements
- undergo an IT security inspection by an IT security inspector with the Public Services and Procurement Canada (PSPC) Contract Security Program (CSP)
- obtain approval in writing from PSPC before protected or classified Government of Canada (GC) information is accessed electronically

Contact us:

Toll-free: 1-866-368-4646
National Capital Region: 613-948-4176
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src

Inspection process

The IT security inspection focuses on the IT systems the organization will be using to produce, process and store protected or classified GC information.

It is conducted **after** the contract has been awarded and physical security requirements have been met.

Before the inspection

1. A PSPC IT inspector is appointed and will contact the organization's CSO.
2. The CSO is required to complete an IT security checklist and submit a detailed picture of its organization's IT environment to the IT security inspector.
3. The IT security checklist is used by the inspector to assess the organization's ability to produce, process and store sensitive government information technology at the organization's work site.

You will be required to complete a new checklist for each contract with IT security requirements.

4. The IT inspector reviews the technical documentation provided by the GC client department. The technical documentation identifies contract specific IT-related requirements and safeguards, which the organization will be required to meet, as part of the GC contract.

Contract IT requirements are generally defined by GC client department's project authorities.

Inspection process cont'd

During the inspection

The IT security inspector evaluates the organization's IT system to ensure that the appropriate safeguards are in place. The organization is expected to demonstrate the ability to securely produce, process and store sensitive GC information.

All personnel working on the contract including IT personnel must be cleared to the appropriate security level.

Only employees who have a **need-to-know** based on their duties are authorized to access sensitive GC information and assets.

Any personnel working on the contract may be interviewed during the IT security inspection.

After the inspection

The recommendations of the IT security inspector must be validated in a **declaration letter** after the inspection is completed.

Once the declaration letter has been received and approved by PSPC's IT security inspector, the organization will be issued an Authority to Process IT approval letter.

The organization can only begin work once PSPC has issued the **approval letter**.

IT approvals are contract-specific, and are valid for the life of the contract.

Return to the Contract Security Program roadmap

Note: Subject to change based on program updates.

Contract Security Program

International industrial security

Reference sheet

International industrial security

Security requirements for international contracts are listed in the:

- request for proposal
- security aspects letter or security requirements checklist (SRCL)
- project/program security instructions

Canadian organizations wanting to bid on foreign government contracts must contact the Public Services and Procurement Canada (PSPC) Contract Security Program (CSP).

International bilateral security instruments

PSPC negotiates international bilateral security instruments with foreign nations.

These instruments promote trade and economic growth and facilitate Canadian industry participation in foreign contracts requiring access to classified information and assets.

Canada has instruments with many countries, such as:

- Australia
- Belgium
- Brazil
- Bulgaria
- Denmark
- Finland
- France
- Germany
- Israel
- Italy
- Netherlands
- New Zealand
- Norway
- South Africa
- Spain
- Sweden
- Switzerland
- United Kingdom
- United States

Contact us:

Toll-free: 1-866-368-4646
National Capital Region: 613-948-4176
Email: ssi-iss@tpsgc-pwgsc.gc.ca
Website: www.tpsgc-pwgsc.gc.ca/esc-src

Visits

Security-cleared individuals are required to get approval to visit an organization in order to discuss or access classified information.

A **request for visit** (RFV) should be made at least **1 to 2 months before** the visit to avoid delays.

PSPC also works with our international counterparts to approve visits to government or contractor sites outside of Canada.

How to get approval

- complete and submit a Request for Visit form RFV form to PSPC CSP
- PSPC will contact the country's designated security authority for processing and approval

For **RFV** to the Department of National Defence (DND) or military sites, please visit our website.

For visits from foreign countries to Canada, foreign organizations must complete and submit a **RFV form** to their own country's designated security authority.

Types of visit requests

One time visit: a single event over a specified period of time, example: a meeting, conference or a symposium

Recurring visit: a series of separate visits for the length of the contract

Emergency visit: reserved for visits of an urgent nature

Request For Visit generic inbox:
ssivisites-.issvisits@tpsgc-pwgsc.gc.ca

Foreign contracts

Foreign organizations wanting to bid on Government of Canada (GC) contracts with security requirements must contact their **designated security authority**, which is the government organization responsible for contract security, in their home country.

North Atlantic Treaty Organization contracts

Organizations wanting to bid on North Atlantic Treaty Organization (NATO) contracts must meet the security requirements described in the solicitation documentation.

International alternative solutions

Customized alternative solutions, based on international best practices, could ensure the safeguarding of protected information handled abroad for the purposes of GC contracting where there is no bilateral security instrument covering protected information.

These alternative solutions depend on the following factors:

- existence of a bilateral security instrument for the exchange of classified information
- location of the foreign suppliers (e.g. within a member of NATO or the European Union)
- nature of information to be shared
- strength of the other country's privacy legislation

An alternative solution uses security clauses to ensure that foreign contractors, including subcontractors, safeguard Canadian protected information according to similar standards as Canadian suppliers.

Transmittal of classified Information

Any classified government information, assets and/or equipment leaving or coming to Canada must be transferred through government-to-government channels.

Return to Contract Security Program roadmap