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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving Public Works and Government Services Canada/Réception des soumissions\Travaux publics et Services gouvernementaux Canada
See herein for bid submission instructions/
Voir la présente pour les instructions sur la présentation d→une soumission
NA
Ontario

Request For Supply Arrangement - Demande pour un arrangement en matière d'approvisionnement

Offer to: Department of Public Works and Government Services

We hereby offer to provide to Canada, as represented by the Minister of Public Works and Government Services, in accordance with the terms and conditions set out herein or attached hereto, the goods, services, and construction detailed herein and on any attached sheets.

Offre au: Ministère des Travaux publics et des Services gouvernementaux

Nous offrons par la présente de fournir au Canada, représenté par le ministre des Travaux publics et des Services gouvernementaux, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici et sur toute feuille ci-annexée.

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Public Works and Government Services / Travaux publics et services gouvernementaux
Kingston Procurement
Des Acquisitions Kingston
86 Clarence Street, 2nd floor
Kingston
Ontario
K7L 1X3

Title - Sujet Defence Intelligence Enterprise

Solicitation No. - N° de l'invitation W6820-21ZZ02/A	**Date** 2022-08-09
Client Reference No. - N° de référence du client W6820-21ZZ02	**GETS Ref. No. - N° de réf. de SEAG** PW-$KIN-655-8682
File No. - N° de dossier KIN-1-56068 (655)	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2022-09-12 Heure Avancée de l'Est HAE

Delivery Required - Livraison exigée
See Herein – Voir ci-inclus

Address Enquiries to: - Adresser toutes questions à: Semple, Patrick	**Buyer Id - Id de l'acheteur** kin655
Telephone No. - N° de téléphone (613)449-3112 ( )	**FAX No. - N° de FAX** (613)545-8067

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
DEPARTMENT OF NATIONAL DEFENCE
P.O. Box 17000 Station Forces
Kingston
Ontario
K7K7B4
Canada

Security - Sécurité
This request for a Supply Arrangement does not include provisions for security.
Cette Demande pour un arrangement ne comprend pas des dispositions en matière de sécurité.

Instructions: See Herein

Instructions: Voir aux présentes

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

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION 3

1.1 Introduction 3
1.2 Summary 3
1.3 Security Requirements 4
1.4 Debriefings 4
1.5 Use of an e-Procurement Solution (EPS) 4

PART 2 - SUPPLIER INSTRUCTIONS 5

2.1 Standard Instructions, Clauses and Conditions 5
2.2 Submission of Arrangements 5
2.3 Former Public Servant - Notification 5
2.4 Federal Contractors Program for Employment Equity - Notification 6
2.5 Enquiries - Request for Supply Arrangements 6
2.6 Applicable Laws 6
2.7 Bid Challenge and Recourse Mechanisms 6

PART 3 - ARRANGEMENT PREPARATION INSTRUCTIONS 7

3.1 Arrangement Preparation Instructions 7

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION 7

4.1 Evaluation Procedures 7
4.2 Basis of Selection 9

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION 9

5.1 Certifications Required with the Arrangement 9
5.2 Certifications Precedent to the Issuance of a Supply Arrangement and Additional Information 10

PART 6 - SUPPLY ARRANGEMENT AND RESULTING CONTRACT CLAUSES 10

A. SUPPLY ARRANGEMENT 10

6.1 Arrangement 10
6.2 Security Requirements 11
6.3 Standard Clauses and Conditions 11
6.4 Term of Supply Arrangement 12
6.5 Authorities 12
6.6 Identified Users 12
6.7 On-going Opportunity for Qualification 12
6.8 Priority of Documents 13
6.9 Certifications and Additional Information 13
6.10 Applicable Laws 13
6.11 Transition to an e-Procurement Solution (EPS) 13

B. BID SOLICITATION 13

6.1 Bid Solicitation Documents 13
6.2 Bid Solicitation Process 14

C. RESULTING CONTRACT CLAUSES 15

6.1 General 15

ANNEX "A" **16**

STATEMENT OF WORK 16

ANNEX "B" **27**

NON DISCLOSURE AGREEMENT 27

ANNEX "C" **28**

SECURITY REQUIREMENTS CHECK LIST 28

ANNEX "D" **29**

CONTRACT SECURITY PROGRAM APPLICATION FOR REGISTRATION (AFR) 29

PART 1 - GENERAL INFORMATION

1.1 Introduction

The Request for Supply Arrangements (RFSA) is divided into six parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Supplier Instructions: provides the instructions applicable to the clauses and conditions of the RFSA;

Part 3 Arrangement Preparation Instructions: provides Suppliers with instructions on how to prepare the arrangement to address the evaluation criteria specified;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria which must be addressed in the arrangement and the basis of selection;

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided; and

Part 6 6A, Supply Arrangement, 6B, Bid Solicitation, and 6C, Resulting Contract Clauses:

6A, includes the Supply Arrangement (SA) with the applicable clauses and conditions;

6B, includes the instructions for the bid solicitation process within the scope of the SA;

6C, includes general information for the conditions which will apply to any contract entered into pursuant to the SA.

The Annexes include the Statement of Work and the Non-disclosure Agreement.

1.2 Summary

1.2.1 The Chief Defence Intelligence (CDI)/Commander Canadian Forces Intelligence Command (CFINTCOM) of the Department of National Defence (DND)/Canadian Armed Forces (CAF) requires a supply arrangement to deliver information technology solutions to support the on-going business evolution of the Defence Intelligence Enterprise (DIE).

The purpose of this supply arrangement is to qualify suppliers who have demonstrated abilities to provide Turnkey High-Assurance On-Premises Information Technology Solutions and on-going in-service support to a variety of Defence Intelligence Enterprise initiatives throughout any of the phases of an initiative development life cycle: Identification, Options Analysis, Definition, Implementation, and transition to In-Service Support.

Supply Arrangements will be issued to all suppliers whose arrangements have been deemed compliant to this RFSA. When DND requires these services, a Request for Proposal (RFP) will be sent to all Supply Arrangement Holders, and will include a technical and financial evaluation.

Services must be provided in accordance with any resultant contract and within the stipulated timeframes.

1.2.2 There are security requirements associated with this requirement. For additional information, consult Part 1 - General Information, and Part 6A - Supply Arrangement. For more information on personnel and organization security screening or security clauses, Suppliers should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website."

1.2.3 This RFSA requires suppliers to use the epost Connect service provided by Canada Post Corporation to transmit their arrangement electronically. Suppliers must refer to Part 2 of the RFSA entitled Supplier Instructions and Part 3 of the RFSA entitled Arrangement Preparation Instructions for further information on using this method.

1.2.4 The Request for Supply Arrangements (RFSA) is to establish supply arrangements for the delivery of the requirement detailed in the RFSA to the Identified Users across Canada, excluding locations within Yukon, Northwest Territories, Nunavut, Quebec, and Labrador that are subject to Comprehensive Land Claims Agreements (CLCAs). Any requirement for deliveries to locations within CLCAs areas within Yukon, Northwest Territories, Nunavut, Quebec, or Labrador will have to be treated as a separate procurement, outside of the resulting supply arrangements."

1.3 Security Requirements

1. Before issuance of a supply arrangement, the following conditions must be met:

   (a) the Supplier must hold a valid organization security clearance as indicated in Part 6A - Supply Arrangement;

2. Before access to sensitive information is provided to the Supplier, the following conditions must be met:

   (a) the Supplier's proposed individuals requiring access to sensitive information, assets or sensitive work sites must meet the security requirements as indicated in Part 6A - Supply Arrangement.

   (b) the Supplier's security capabilities must be met as indicated Part 6A - Supply Arrangement.

3. For additional information on security requirements, Suppliers should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

1.4 Debriefings

Suppliers may request a debriefing on the results of the request for supply arrangements process. Suppliers should make the request to the Supply Arrangement Authority within 15 working days of receipt of the results of the request for supply arrangements process. The debriefing may be in writing, by telephone or in person.

1.5 Use of an e-Procurement Solution (EPS)

Canada is currently developing an online EPS for faster and more convenient ordering of goods and services. In support of the anticipated transition to this system and how it may impact any resulting Supply Arrangement that is issued under this solicitation, refer to 6.12 Transition to an e-Procurement Solution (EPS).

The Government of Canada's press release provides additional information.

PART 2 - SUPPLIER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the Request for Supply Arrangements (RFSA) by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

Suppliers who submit an arrangement agree to be bound by the instructions, clauses and conditions of the RFSA and accept the clauses and conditions of the Supply Arrangement and resulting contract(s).

The 2008 (2022-01-28) Standard Instructions - Request for Supply Arrangements - Goods or Services, are incorporated by reference into and form part of the RFSA.

Subsection 5.4 of 2008, Standard Instructions - Request for Supply Arrangements - Goods or Services, is amended as follows:

Delete: 60 days
Insert: 240 days

2.2 Submission of Arrangements

Arrangements must be submitted only to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated in the RFSA.

PWGSC Ontario Region Bid Receiving Unit
Only arrangements submitted using epost Connect service will be accepted. The Supplier must send an email requesting to open an epost Connect conversation to the following address:
TPSGC.orreceptiondessoumissions-orbidreceiving.PWGSC@tpsgc-pwgsc.gc.ca

Note: Arrangements will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2008, or to send arrangements through an epost Connect message if the Supplier is using its own licensing agreement for epost Connect.

It is the Supplier's responsibility to ensure the request for opening an epost Connect conversation is sent to the email address above at least six days before the Request for Supply Arrangements closing date.

Transmission of arrangements by facsimile or hardcopy to PWGSC will not be accepted

2.3 Former Public Servant - Notification

Service contracts awarded to former public servants in receipt of a pension or a lump sum payment must bear the closest public scrutiny and reflect fairness in the spending of public funds. Therefore, the bid solicitation will require that you provide information that, were you to be the successful bidder, your status with respect to being a former public servant in receipt of a pension or a lump sum payment, will be required to report this information on the departmental websites as part of the published proactive disclosure reports generated in accordance with Treasury Board policies and directives on contracts with

former public servants, Contracting Policy Notice 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

2.4 Federal Contractors Program for Employment Equity - Notification

The Federal Contractors Program (FCP) for employment equity requires that some contractors make a formal commitment to Employment and Social Development Canada (ESDC) - Labour to implement employment equity. In the event that this Supply Arrangement would lead to a contract subject to the Federal Contractors Program (FCP) for employment equity, the bid solicitation and resulting contract templates would include such specific requirements. Further information on the Federal Contractors Program (FCP) for employment equity can be found on Employment and Social Development Canada (ESDC) - Labour's website.

2.5 Enquiries - Request for Supply Arrangements

All enquiries must be submitted in writing to the Supply Arrangement Authority no later than 5 calendar days before the Request for Supply Arrangements (RFSA) closing date. Enquiries received after that time may not be answered.

Suppliers should reference as accurately as possible the numbered item of the RFSA to which the enquiry relates. Care should be taken by Suppliers to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that Suppliers do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered to all Suppliers. Enquiries not submitted in a form that can be distributed to all Suppliers may not be answered by Canada.

2.6 Applicable Laws

The Supply Arrangement (SA) and any contract awarded under the SA must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

Suppliers may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of the arrangement, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Suppliers.

2.7 Bid Challenge and Recourse Mechanisms

(a) Several mechanisms are available to potential suppliers to challenge aspects of the procurement process up to and including contract award.

(b) Canada encourages suppliers to first bring their concerns to the attention of the Contracting Authority. Canada's Buy and Sell website, under the heading "Bid Challenge and Recourse Mechanisms" contains information on potential complaint bodies such as:

- Office of the Procurement Ombudsman (OPO)
- Canadian International Trade Tribunal (CITT)

(c) Suppliers should note that there are **strict deadlines** for filing complaints, and the time periods vary depending on the complaint body in question. Suppliers should therefore act quickly when they want to challenge any aspect of the procurement process.

PART 3 - ARRANGEMENT PREPARATION INSTRUCTIONS

3.1 Arrangement Preparation Instructions

- If the Supplier chooses to submit its arrangement electronically, Canada requests that the Supplier submits its arrangement in accordance with section 08 of the 2008 standard instructions. The CPC Connect system has a limit of 1GB per single message posted and a limit of 20GB per conversation.

  Canada requests that the arrangement be gathered per section and separated as follows:

  Section I: Technical Arrangement
  Section II: Certifications

Section I: Technical Arrangement
In the technical arrangement, Suppliers should explain and demonstrate how they propose to meet the requirements and how they will carry out the Work.

Section II: Certifications
Suppliers must submit the certifications and additional information required under Part 5.

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) Arrangements will be assessed in accordance with the entire requirement of the Request for Supply Arrangements including the technical and financial evaluation criteria.

(b) An evaluation team composed of representatives of Canada will evaluate the arrangements.

4.1.1 Technical Evaluation

4.1.1.1 Mandatory Technical Criteria

Bidders must meet the following mandatory criteria to be considered for the award of a Supply Arrangement.

Number	Requirement	Submission Requirements
MT1	The Bidder must consent to the non-disclosure requirements specified in Annex B of the RFP	The Bidder must complete and sign the nondisclosure agreement in Annex B of the RFP
MT2	The Bidder must demonstrate experience in the design, development and delivery of a minimum of 2 Turnkey High-Assurance On-Premises information technology solutions. Each solution must have: a) Had a value of at least $1 million; and	The Bidder must provide a project description that demonstrates the all requirements were met. Additionally, the bidder must provide the organization name and current contact information of a client reference who can validate the information provided.

	b) Been completed within the past 5 years as of bid closing.	
MT3	The Bidder must demonstrate that it has implemented designed, developed and implemented a Turnkey High-Assurance On-Premises information technology solutions for a defence, security or intelligence agency of Canada or its closest Five Eyes Allies (United States, United Kingdom, Australia or New Zealand).	The Bidder must provide a project description that demonstrates the all requirements were met. Additionally, the bidder must provide the organization name and current contact information of a client reference who can validate the information provided. NOTE: This reference may be one of the projects provided in response to M2
MT4	The Bidder must demonstrate that it has completed all activities to maintain Supply Chain Integrity, including Acquisition and Procurement Activities, Shipping and Transportation, On Delivery, Post Delivery, and Disposal, Close-out and Decommissioning Activities (all elements of paragraph 5.3.1 through 5.3.5).	The Bidder must provide a project description that demonstrates that all requirements were met. Additionally, the bidder must provide the organization name and current contact information of a client reference who can validate the information provided. NOTE: This reference may be one of the projects provided in response to M2 or M3
MT5	M 1. In its responses to M2 and M3, the Bidder must demonstrate that it has designed developed and implemented solutions that incorporated a minimum of 5 of the following: a. Infrastructure as a Service (IaaS); b. Platform as a Service (PaaS); c. Back-up as a Service (BaaS); d. Disaster Recovery as a Service (DRaaS) and container services; e. Software as a Service (SaaS); f. Identity and Access Management services, enabling a multi-tenant virtualized information technology environment within information technology servers and services;	The Bidder must provide a project description that demonstrates that the specified solutions were designed developed and implemented.

	g. Transportable and deployable temporary Information Technology services; h. Ancillary equipment and peripherals to support managed print and scanning services, unified telecommunications and audio/video conferencing systems; and i. Solutions and systems for data analytics.	
MT6	The Bidder must demonstrate that it has established practices, processes and methodologies governing the solution design and development activities that align with industry best practices such as CMMI, ISO or Agile.	The bidder must provide relevant documentation and/or industry certifications or accreditations.

Canada may contact the Supplier`s references for MT2, MT3, MT4, by phone or email within 7 calendar days of the bid closing to verify the details provided by the Supplier. Canada may not accept the Supplier's submission if the details are not verified by the associated references.

4.2 Basis of Selection

An Arrangement must comply with the requirements of the Request for Supply Arrangements and meet all mandatory technical criteria to be declared responsive.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Suppliers must provide the required certifications and additional information to be issued a supply arrangement (SA).

The certifications provided by Suppliers to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare an arrangement non-responsive, or will declare a contractor in default if any certification made by the Supplier is found to be untrue whether made knowingly or unknowingly during the arrangement evaluation period, or during the period of any supply arrangement arising from this RFSA and any resulting contracts.

The Supply Arrangement Authority will have the right to ask for additional information to verify the Supplier's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Supply Arrangement Authority will render the arrangement non-responsive or constitute a default under the Contract.

5.1 Certifications Required with the Arrangement

Suppliers must submit the following duly completed certifications as part of their arrangement.

5.1.1 Integrity Provisions - Declaration of Convicted Offences

In accordance with the Integrity Provisions of the Standard Instructions, all suppliers must provide with their arrangement, **if applicable**, the declaration form available on the Forms for the Integrity Regime website (http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html), to be given further consideration in the procurement process.

5.2 Certifications Precedent to the Issuance of a Supply Arrangement and Additional Information

The certifications and additional information listed below should be submitted with the arrangement but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Supply Arrangement Authority will inform the Supplier of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame provided will render the arrangement non-responsive.

5.2.1 Integrity Provisions – Required Documentation

In accordance with the section titled Information to be provided when bidding, contracting or entering into a real property agreement of the Ineligibility and Suspension Policy (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html), the Supplier must provide the required documentation, as applicable, to be given further consideration in the procurement process.

5.2.2 Additional Certifications Precedent to Issuance of a Supply Arrangement

5.2.2.1 Security Requirements – Required Documentation

In accordance with the requirements of the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html), the Offeror must provide a completed Application for Registration (AFR) form to be given further consideration in the procurement process.

Offerors are reminded to obtain the required security clearance and, as applicable, security capabilities promptly. As indicated above, offerors who do not provide all the required information at bid closing will be given the opportunity to complete any missing information from the AFR form within a period set by the Contracting Authority. If that information is not provided within the timeframe established by the Contracting Authority (including any extensions granted by the Contracting Authority in its discretion), or if Canada requires further information from the Offeror in connection with assessing the request for security clearance (i.e., information not required by the AFR), the Offeror will be required to submit that information within the time period established by the Contracting Authority, which will not be less than 48 hours. If, at any time, the Offeror fails to provide the required information within the timeframe established by the Contracting Authority, its bid will be declared non-compliant.

5.2.2.2 Non-Disclosure Agreement

Suppliers must provide a signed Non-Disclosure Agreement in accordance with Annex “B”. If it is not submitted with the arrangement, it must be provided within 2 days of the request from the Supply Arrangement Authority.

PART 6 - SUPPLY ARRANGEMENT AND RESULTING CONTRACT CLAUSES

A. SUPPLY ARRANGEMENT

6.1 Arrangement

The Supply Arrangement covers the Work described in the Statement of Work at Annex “A’”

6.2 Security Requirements

6.2.1 The following security requirements (SRCL and related clauses provided by the Contract Security Program) apply and form part of the Supply Arrangement.

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:
PWGSC FILE No. W6820-21-ZZ02

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Facility Security Clearance at the level of TOP SECRET or NATO SECRET, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

2. The Contractor/Offeror personnel requiring access to CLASSIFIED/PROTECTED information, assets or sensitive site(s) **must be a citizen of Canada** must EACH hold a valid personnel security screening at the level of TOP SECRET SIGINT, TOP SECRET, NATO SECRET or SECRET, as required, granted or approved by the CSP, PWGSC.

3. The Contractor personnel requiring access to NATO RESTRICTED information or assets **must be a citizen of Canada** and EACH hold a valid TOP SECRET SIGINT or its equivalent, granted or approved by the appropriate delegated NATO Security Authority.

4. The Contractor/Offeror personnel requiring access to NATO CLASSIFIED information, assets or sensitive site(s) **must be a citizen Canada** and EACH hold a valid personnel security screening at the level of NATO SECRET , granted or approved by the appropriate delegated NATO Security Authority.

5. The Contractor/Offeror MUST NOT remove any CLASSIFIED/PROTECTED information or assets from the identified site(s), and the Contractor/Offeror must ensure that its personnel are made aware of and comply with this restriction.

6. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the CSP, PWGSC.

7. The Contractor/Offeror must comply with the provisions of the:

   (a) Security Requirements Check List and security guide (if applicable), attached at Annex ____;
   (b) *Contract Security Manual* (Latest Edition).

6.3 Standard Clauses and Conditions

All clauses and conditions identified in the Supply Arrangement and resulting contract(s) by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

6.3.1 General Conditions

2020 (2022-01-28) General Conditions - Supply Arrangement - Goods or Services, apply to and form part of the Supply Arrangement.

6.4 Term of Supply Arrangement

6.4.1 Period of the Supply Arrangement

The period for awarding contracts under the Supply Arrangement is from issuance to March 2026.

6.4.2 Comprehensive Land Claims Agreements (CLCAs)

The Supply Arrangement (SA) is for the delivery of the requirement detailed in the SA to the Identified Users across Canada, excluding locations within Yukon, Northwest Territories, Nunavut, Quebec, and Labrador that are subject to Comprehensive Land Claims Agreements (CLCAs). Any requirement for deliveries to locations within CLCAs areas within Yukon, Northwest Territories, Nunavut, Quebec, or Labrador will have to be treated as a separate procurement, outside of the supply arrangement.

6.5 Authorities

6.5.1 Supply Arrangement Authority

The Supply Arrangement Authority is:

Name: Patrick Semple
Title: Supply Specialist
Public Works and Government Services Canada
Acquisitions Branch
Directorate: Acquisitions Kingston
86 Clarence Street, 2nd Floor
Kingston, Ontario K7L 1X3

Telephone: 613 530-3117
E-mail address: patrick.semple@pwgsc-tpsgc.gc.ca

The Supply Arrangement Authority is responsible for the issuance of the Supply Arrangement, its administration and its revision, if applicable.

6.5.2 Supplier's Representative

Name: _____
Title: _____
Organization: _____
Address: _____

Telephone: ___ ___ _____
Facsimile: ___ ___ _____
E-mail address: _____

6.6 Identified Users

The Identified User is: CFINTCOM (DND).

6.7 On-going Opportunity for Qualification

A Notice will be posted once a year on the Government Electronic Tendering Service (GETS) to allow new Suppliers to become qualified. Existing qualified Suppliers, who have been issued a supply arrangement, will not be required to submit a new arrangement.

6.8 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

(a) the articles of the Supply Arrangement;
(b) the general conditions 2020 (2022-01-28), General Conditions - Supply Arrangement - Goods or Services;
(c) Annex A, Statement of Work;
(d) Annex B, Non Disclosure Agreement;
(e) the Supplier's arrangement dated _____

6.9 Certifications and Additional Information

6.9.1 Compliance

Unless specified otherwise, the continuous compliance with the certifications provided by the Supplier in its arrangement or precedent to issuance of the Supply Arrangement (SA), and the ongoing cooperation in providing additional information are conditions of issuance of the SA and failure to comply will constitute the Supplier in default. Certifications are subject to verification by Canada during the entire period of the SA and of any resulting contract that would continue beyond the period of the SA.

6.10 Applicable Laws

The Supply Arrangement (SA) and any contract resulting from the SA must be interpreted and governed, and the relations between the parties determined, by the laws in force in _____

6.11 Transition to an e-Procurement Solution (EPS)

During the period of the Supply Arrangement, Canada may transition to an EPS for more efficient processing and management of individual contracts for any or all of the SA's applicable goods and services. Canada reserves the right, at its sole discretion, to make the use of the new e-procurement solution mandatory.

Canada agrees to provide the Supplier with at least a three-month notice to allow for any measures necessary for the integration of the Supply Arrangement into the EPS. The notice will include a detailed information package indicating the requirements, as well as any applicable guidance and support.

If the Supplier chooses not to provide the supply arrangement of their goods or services through the e-procurement solution, the Supply Arrangement may be set aside by Canada.

B. BID SOLICITATION

6.1 Bid Solicitation Documents

Canada will use the following bid solicitation templates based on the estimated dollar value and complexity of the requirement:

- Medium Complexity (MC) for medium complexity requirements;
- High Complexity (HC) for more complex requirements.

A copy of the standard procurement template(s) can be requested by suppliers from the Supply Arrangement Authority or the Contracting Authority, as applicable.

Note: References to the HC and MC in PWGSC Requests for Supply Arrangements are provided as examples only. The latest versions of the template and terms and conditions will be used at time of bid solicitation.

The bid solicitation will contain as a minimum the following:

(a) security requirements (*if applicable*);

(b) a complete description of the Work to be performed;

(c) 2003, Standard Instructions - Goods or Services - Competitive Requirements; ***OR*** 2004, Standard Instructions - Goods or Services - Non-competitive Requirements;

Subsection 3.a) of Section 01, Integrity Provisions - Bid of the Standard Instructions (insert, as applicable: 2003 or 2004) incorporated by reference above is deleted in its entirety and replaced with the following:

a. at the time of submitting an arrangement under the Request for Supply Arrangements (RFSA), the Bidder has already provided a list of names, as requested under the *Ineligibility and Suspension Policy*.During this procurement process, the Bidder must immediately inform Canada in writing of any changes affecting the list of directors."

(d) bid preparation instructions;

(e) instructions for the submission of bids (address for submission of bids, bid closing date and time);

(f) evaluation procedures and basis of selection;

(g) certifications*;*

- **Federal Contractors Program (FCP) for Employment Equity - Notification**

- SACC Manual A3005T, A3010T for service requirements when specific individuals will be proposed for the work*;*

- **Integrity Provisions - Declaration of Convicted Offences*;***

(i) conditions of the resulting contract.

6.2 Bid Solicitation Process

6.2.1 Bids will be solicited for specific requirements within the scope of the Supply Arrangement (SA) from Suppliers who have been issued a SA.

6.2.2 The bid solicitation will be sent directly to Suppliers.

(a) A RFP will be sent to all Supply Arrangement Holders, which will include a technical and financial evaluation; and

(b) PWGSC will be responsible for the solicitation process and the award of any resultant contract(s).

C. RESULTING CONTRACT CLAUSES

6.1 General

The conditions of any contract awarded under the Supply Arrangement will be in accordance with the resulting contract clauses of the template used for the bid solicitation.

For any contract to be awarded using the template:

(a) **MC** (for medium complexity requirements), general conditions 2020 will apply to the resulting contract;

(b) **HC** (for high complexity requirements), general conditions 2032 will apply to the resulting contract.

A copy of the template(s) can be provided upon request by contacting the Strategic Policy Integration Division by sending a query to TPSGC.Outilsdapprovisionnement-ProcurementTools.PWGSC@tpsgc-pwgsc.gc.ca.

Note: References to the HC, MC and Simple templates in PWGSC Requests for Supply Arrangements are provided as examples only. The latest versions of the template and terms and conditions will be used at time of bid solicitation.

ANNEX "A"

STATEMENT OF WORK

1 REQUIREMENT

1.1 The Chief Defence Intelligence (CDI)/Commander Canadian Forces Intelligence Command (CFINTCOM) of the Department of National Defence (DND)/Canadian Armed Forces (CAF) requires a supply arrangement to deliver information technology solutions to support the on-going business evolution of the Defence Intelligence Enterprise (DIE).

1.2 Appendix B provides a Glossary and explains key terms used throughout this SOW

2 BACKGROUND

2.1 Within the DND/CAF, the Defence Intelligence Enterprise (DIE) consists of all defence intelligence programmes, administration and activities across the DND/CAF, including all operations. Specifically, the DIE includes all personnel, resources and assets within the DND/CAF that work together to deliver credible, timely and integrated defence intelligence capabilities, products and services to the DND/CAF, Government of Canada and Allies in support of Canada's national security objectives.

2.2 The DIE is led by Chief Defence Intelligence (CDI)/Commander Canadian Forces Intelligence Command (CFINTCOM). It also includes elements of the DND/CAF (such as some elements within Royal Canadian Navy, Canadian Army, Royal Canadian Air Force, Canadian Special Forces Command, Canadian Joint Operations Command, Assistance Deputy Minister (Information Management) and Strategic Joint Staff) that have direct or indirect supporting roles in the direction, collection, processing and dissemination of defence intelligence products, at home and abroad.

2.3 Fundamentally, the business of the DIE is the efficient and effective delivery of:

“credible, timely and integrated defence intelligence capabilities, products and services to the DND and the CAF, Government of Canada and Allies in support of Canada's national security objectives.”

2.4 The Director General Intelligence Enterprise (DGIE), along with the Director Intelligence Information Management (D Int IM), within CFINTCOM are responsible for developing and managing the execution of force development activities within the DIE, including the analysis, experimentation and validation of intelligence capabilities, enablers and force structures to be integrated and implemented into the Canadian Armed Forces, while ensuring interoperability with our domestic and international allies and partners. The DGIE, supported by D Int IM Directorate, provides focused expertise to develop and introduce new capabilities and resource capacities, develops and integrates new knowledge from internal and external sources through research and experimentation, assesses the future operating and security environments, develops new concepts and doctrine that provide operational advantage to joint military activities, develops individual and collective training programs and manages project requirements. In short, the DGIE group and the D Int IM Directorate are actively engaged in the on-going business evolution of the DIE to maintain pace with modern technology and operational requirements.

3 SCOPE

3.1 The purpose of this supply arrangement is to qualify suppliers who have demonstrated abilities to provide Turnkey High-Assurance On-Premises Information Technology Solutions and on-going in-service support to a variety of Defence Intelligence Enterprise initiatives throughout any of the

phases of an initiative development life cycle: Identification, Options Analysis, Definition, Implementation, and transition to In-Service Support.

3.2 The specific requirements and deliverables of these technology solutions will be defined in subsequent Statements of Work that will be issued in subsequent Requests for Proposals issued to qualified suppliers. The work could include the Design, Development, Procurement, Assembly, Configuration, Installation, Training, Documentation and In-Service Support of technology solutions such as:

a. Solutions and systems for On-Premises Infrastructure as a Service (IaaS);
b. Solutions and systems for On-Premises Back-up as a Service (BaaS);
c. Solutions and systems for On-Premises Disaster Recovery as a Service (DRaaS) and container services;
d. Solutions and systems for On-Premises Software as a Service (SaaS);
e. Solutions and Systems for On-Premises Identity and Access Management services;
f. enabling a multi-tenant virtualized information technology environment within information technology servers and services;
g. Solutions and systems for Deployable Information Technology services;
h. Solutions and systems for On-Premises ancillary equipment and peripherals to support managed print and scanning services, unified telecommunications and audio/video conferencing systems; and
i. Solutions and systems for data analytics.

3.3 All supplied solutions must meet the Supply Chain Integrity provisions specified in Section 5.

3.4 To the greatest extent possible, these solutions will leverage technologies that are currently employed by Canada's closest Allies and other Government of Canada departments and agencies.

3.5 The contractor will be required to provide a robust project management and system engineering capabilities to help ensure the timely delivery of high-quality solutions that meet all specified operational, performance and technical requirements.

3.6 In addition to providing solutions, the Contractor may also be required to provide a complete range of integrated logistics support items which could include operator and maintainer documentation, technical data and drawings, configuration management documentation and training services.

4 TASKS AND DELIVERABLES

4.1 The specific tasks and deliverables for each solution requested will be defined with the associated Statements of Work that will be issued as part of Requests for Proposal that will be issued to qualified Supply Arrangement holders. Deliverables could include IT hardware and peripherals, software and firmware and/or design, development, installation, configuration, customization and technical support services.

4.2 Documentation must be submitted to the Technical Authority in English. The Technical Authority will be responsible for the review and acceptance of all deliverables.

4.3 All documentation deliverables must be provided in one (1) hard copy and one (1) soft copy, presented in a format acceptable to the TA. The soft copy must be compatible with Microsoft Office 2013 or later, or Adobe Reader XI or later.

5 SUPPLY CHAIN INTEGRITY

5.1 Although information technology and assets do not necessarily constitute Defence Intelligence, they will have a foundational effect on the vulnerability of the DIE as a whole, and the overall

manner of the conduct of information security within the DIE. In short, information technology and assets are part of the Supply Chain of the DIE and must be treated accordingly.

5.2 Supply Chain Integrity (SCI) is the process of managing an organization's internal capabilities, as well as its partners and suppliers, to ensure all elements of an integrated solution are of high-assurance. It includes not just the supply chain of equipment, hardware and software but all the supply of Contracted Professional Services (personnel and support services) and organization personnel.

5.3 For each statement of work issued under the performance, there will be specific policies, standards and procedures defined that will form a part of the essential deliverable requirements. These include:

5.3.1 Acquisition and Procurement Activities

a. General:

1) In consultation with and the approval of the TA, all procurements shall engage an appropriate Supply Chain Risk Assessment process to assess each procurement for supply chain threats and recommend the appropriate risk response measures,

2) General Terms and Conditions of all procurements shall include, where appropriate, security requirements tailored to meet the overall security requirements concerning:

i. **Transmission of Sensitive Data:** to deal with concerns regarding the transmission of data, especially when the data is considered sensitive, such as ITI Information and Assets,

ii. **Security Clearance and Escorting of Personnel**: to deal with concerns regarding security clearance of contractor personnel who have access to system facilities, equipment, or data,

iii. **Subcontracting**: to deal with concerns regarding situations where the Prime Contractor is not performing all of the work and there is a need to approve subcontractors for supply chain reasons,

iv. **Product Assurance and Equipment and Inventory:** to ensure Canada has a complete list of equipment in use for delivery of the services. The approach shall be that, whenever possible, only Common Criteria (CC) certified and Crypto Module Validation Program (CMVP) validated products are trusted. The certification requirements shall be listed in the mandatory evaluation criteria or in the specification,

v. **Location of Databases, Network Traffic Routing, and Data**: to ensure Canada has control over the location of databases, network traffic and data, where there is concern with certain jurisdictions or the laws of a certain jurisdiction. This includes Project Information and Assets, budgets, contract deliverables, etc.,

vi. **Network Connectivity and Access Control:** to ensure that there are controls in place to deal with authorized vs. unauthorized access to Canada's network(s) and database(s), including Project Information and Assets held with the Contractor,

vii. **Vulnerability Assessment and Management:** to ensure that Canada, in a timely manner, is informed of vulnerabilities in the Contractor supplied equipment and that the Contractor will take corrective actions,

viii. **Resilience of Supply Chain and Disaster Recovery Plan**: to deal with business continuity and disaster recovery,
ix. **Physical Security:** to deal with physical security requirements applicable to Contractors premises when necessary,
x. **Threat and Risk Assessment**: to deal with Threats and Risks that could compromise Canada's networks or the services being delivered by the Contractor. This clause would be in addition to the Threat and Risk Assessment (TRA) required for accreditation of a system,
xi. **Security Monitoring and Incident Reporting:** to deal with abnormal and unauthorized use of the network,
xii. **Security Audit**: to allow Canada to audit the Contractor's compliance with the security requirements in service contracts, and
xiii. **Change in Control:** to require the Contractor to seek approval from Canada and Canadian and International Industrial Security Directorate (CISD) for a change in control. From a security perspective, it is expected that some contracts will require consent from Canada for a change in control;

b. Tendering:

1) On Tendering, project names and end-use shall not be disclosed. The tendering process shall be in a manner that does not allow deduction of a project name, user organization, nor system end use;
2) Communications with Vendors and Suppliers shall be conducted in a manner to mask the end-use, CDI and CFINTCOM from the communications;
3) End-use information shall be restricted on a need-to-know basis and only released to Vendors or Suppliers with the appropriate Facility Security Clearance;
4) No grey market solutions will be used or acquired; and
5) Tendering and Supplier selection shall be based on the recommended risk response measures provided by the TA, and, when applicable, considering specific restrictions on suppliers that may originate from our allies.

5.3.2 Shipping and Transportation:

a. Packaging and marking shall never identify end-use titles, CDI, CFINTCOM, nor any other name that can be easily linked with the CAF;
b. Contract delivery times shall be shortest time possible to minimize risk of compromise;
c. Where appropriate, only Trusted couriers and shipping agents (as defined by CISD) shall be used;
d. Where appropriate, delivery routes shall be coordinated in advance to select the most direct route to avoid risk of compromise; and
e. Detailed handling and transaction chain of custody records shall be required from the vendor or supplier with each delivery.

5.3.3 On Delivery:

a. On Receiving products or goods within DND and the CAF, all project assets shall be immediately received and stored in secure storage rooms in accordance with instructions issued by the TA,
b. All hardware and software shall be inspected and examined in accordance with instructions issued by the TA as soon as possible upon delivery,
c. Chain of custody records during transportation shall be inspected and audited by the contractor and provided to the TA,
d. Custody records shall be maintained and updated by the Contractor from moment of receipt until final disposition within the IT systems and the CMDB updated.

5.3.4 Post Delivery: The Contractor shall continue to review and track the provenance, to an appropriate level, of raw materials, components, and subassemblies as they move throughout the supply chain via tagging, or some other methods. This will include updating and management of a detailed Configuration Management Database (CMDB) that tracks all key data elements of the Information Technology and Assets,

a. reporting security incidents to the TA, as appropriate,
b. on-going evaluation of the effectiveness of supply chain security controls, reporting on the achievement of security control objectives to the TA and recommend corrective action to address deficiencies identified in performance measurement and evaluations,
c. Ensure all solutions implemented by an activity or project have been fully integrated within the security framework of the DIE to ensure an effective on-going security posture, including routine security processes, procedures, controls, monitoring, reviews, inspections, and audits will be in place at all times.

5.3.5 Disposal, Close-out and Decommissioning Activities. On Disposal, Close-out and Decommissioning of some or all aspects of system components, a risk assessment shall be conducted to determine the most appropriate Disposal, Close-out or Decommissioning solution. The TA shall be consulted in advance to determine the appropriate methods or risk response measures before proceeding.

6 ADDITIONAL CONSTRAINTS

6.1 For all Systems and Solutions contracted for On-Premises installation and operation, DND, through the TA, will define the in the contract the exact location for installation, the electrical power and HVAC capacities, network connectivity and all other elements necessary to permit the Contractor to install the required systems to achieve their contracted performance requirements.

6.2 Access to DND facilities on weekends and holidays requires prior arrangement and approval from the TA.

6.3 DND facilities are restricted areas and the use of electronic devices including cell phones, cameras or any other electronic recording device are not allowed.

6.4 It is the responsibility of the Contractor to have an approved Visit Clearance Request (VCR) prior to the start of work, subject to a waiver at the discretion of the Technical Authority.

6.5 Throughout the performance of the work the Contractor’s personnel will have access to computer networks and certain electronic equipment which are deemed to be Controlled Goods. The Contractor personnel must be registered with the CISD Branch of PWGSC.

6.6 Occasionally resources must handle objects weighing up to 30kg using additional resources if required (i.e. two-man lift). For instances where total combined objects weight more than 30kg, assistance will be provided by GNS personnel and/or material handling equipment like pallet jacks and hand trucks will be made available.

6.7 Completion of some of the tasks will require the Contractor personnel participate in meetings, workshops and requirements gathering activities which will occur during normal working hours which are between 0700hrs and 1600hrs. The working week is five (5) days, Monday to Friday.

7 LOCATION OF WORK

7.1 The completion of some tasks may require Contractor personnel to be present at DND facilities, primarily at 101 Colonel By Drive, Ottawa Ontario or at other locations throughout the NCR to attend meetings, access computer systems and databases or

conduct research. Any other activities may be conducted at the Contractor facilities using Contractor equipment.

7.2 DND will provide the Contractor with DND/CAF documents as required to successfully accomplish the assigned tasks. The Contractor must perform the work in accordance with the DND/CAF approved version of these documents.

7.3 DND/CAF will provide terminals for system access to perform necessary functions, as well as a workspace in which to conduct specific tasks that must be carried out within DND/CAF facilities due to the nature and classification of work involved.

8 TRAVEL REQUIREMENTS

8.1 Travel may be required in the completion of certain tasks. Every occurrence of travel must be authorized in writing by the Technical Authority.

8.2 The Contractor will be reimbursed for authorized travel costs reasonably incurred in the performance of the Work in accordance with the National Joint Council Travel Directive (http://www.njc-cnm.gc.ca/directive/travel-voyage/index-eng.php).

8.3 Travel to DND facilities within the NCR will not be reimbursed.

9 LANGUAGE REQUIREMENTS

9.1 The Contractor resources must be fluent in English. For the purposes of this requirement, a resource will be considered to speak a language fluently if the resource can:

a. Give detailed explanations and descriptions;
b. Handle hypothetical questions;
c. Support an opinion, defend a point of view or justify an action; and
d. Counsel and give advice.

10 TECHNICAL AUTHORITY (TA)

10.1 The Technical Authority for all requirements will be the primary point of contact for Contractor personnel and will be stated in the Contract award document. All reports, deliverables, documentation and services rendered will be subject to inspection and acceptance by the Technical Authority or his/her designated representative.

APPENDIX B: GLOSSARY

Term	Description
Appropriate	[adjective] suitable or proper in the circumstances. [Oxford English Dictionary]
asset	Tangible or intangible things of the Government of Canada. Assets include, but are not limited to, information in all forms and media, networks, systems, material, real property, financial resources, employee trust, public confidence and international reputation. [DTB 46707]
Assurance	means the confidence that a system or product or feature of a system or product is free from vulnerability [DTB 12432]
Assurance Evidence	The information upon which decision regarding assurance, trustworthiness, and risk of the solution are substantiated. Note: Assurance evidence is specific to an agreed set of claims. The security perspective focuses on assurance evidence for security-relevant claims whereas other engineering disciplines may have their own focus (e.g. safety). [NIST SP 800-160]
Authority	means the legal right to make decisions, transmit intentions to subordinate commanders, and impose one's will on subordinates [DTB 21091]
Availability	The state of being accessible and usable in a timely and reliable manner.
Backup as a service (BaaS)	Backup as a service (BaaS) is an approach to backing up data that involves purchasing backup and recovery services from an online data backup provider. Instead of performing backup with a centralized, on-premises IT department, BaaS connects systems to a private, public or hybrid cloud managed by the outside provider. https://searchdatabackup.techtarget.com/definition/backup-as-a-service-BaaS
Chain of Custody	the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of the components within a supply chain.
Confidentiality	A characteristic applied to information to signify that it can only be disclosed to authorized individuals to prevent injury to national or other interests.
data analytics	The term "**data analytics**" refers to the process of examining datasets to draw conclusions about the information they contain. Data analytic techniques enable businesses to take raw business data and uncover patterns to extract valuable insights from it regarding the nature of their business.
Defence Intelligence	All intelligence from the tactical to the strategic level in support of military operations and planning. [DTB Record 47286]
Defence Intelligence Enterprise	The Defence Intelligence Enterprise (DIE) consists of all defence intelligence programmes, administration and activities across the DND and the CAF, including all operations. Specifically, the DIE includes all personnel, resources and assets within the DND and the CAF that work together to deliver credible, timely and integrated defence intelligence capabilities, products and services to the DND and the CAF, Government of Canada and Allies in support of Canada's national security objectives.

Term	Description
Deployable Information Technology services	Deployable Information Technology services refers to On-premises solutions where the On-premises location will be temporary in nature and often installed under harsh and austere conditions. The equipment will usually require some degree of ruggedization and electronic emission controls (TEMPEST) for security reasons. Deployable solutions may range in complexity from a standalone ruggedized laptop computer to 2 or 3 computers networked together in a small field office to 10 to 20 computers networked together in a large field office with local central domain and files servers. Generally, deployable solutions will be limited to solutions that can be carried (one component at a time), assembled and configured on site by no more than two people.
Disaster recovery as a service (DRaaS)	Disaster recovery as a service (DRaaS) is the replication and hosting of physical or virtual servers by a third party to provide failover in the event of a natural catastrophe, power outage or another type of business disruption. https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-as-a-service-DRaaS
Grey Market	goods are legal, non-counterfeit goods sold outside normal distribution channels by entities that may have no relationship with the producer of the goods. This form of parallel import frequently occurs when the price of an item is significantly higher in one country than another. Grey market is very common for electronic equipment.
High-Assurance	High-Assurance systems are built in such a way that it is possible to prove with mathematical certainty that they work precisely as intended and as designed. These systems provide clear, digital evidence that can be checked by third parties to prove that they work exactly as intended – no more, no less. [FreeandFair.US]
Identity and Access Management	Identity management (IdM), also known as identity and access management (IAM or IdAM), is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. IdM systems fall under the overarching umbrellas of IT security and data management. Identity and access management systems not only identify, authenticate, and authorize individuals who will be utilizing IT resources, but also the hardware and applications employees need to access. Identity and access management solutions have become more prevalent and critical in recent years as regulatory compliance requirements have become increasingly more rigorous and complex. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements. The terms "identity management" (IdM) and "identity and access management" are used interchangeably in the area of identity access management. Identity-management systems, products, applications and platforms manage identifying and ancillary data about entities that include individuals, computer-related hardware, and software applications. IdM covers issues such as how users gain an identity, the roles and, sometimes, the permissions that identity grants, the protection of that identity and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.). https://en.wikipedia.org/wiki/Identity_management
information	Unprocessed data of every description which may be used in the production of intelligence. [DTB 18621]

Term	Description
Information Security	The protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. Note: Information may exist in the human mind, in document form and in electronic form. Information in the human mind will be protected by the use of appropriate personnel security measures. Information in document form will be protected by the use of appropriate document security measures. Information in electronic form will be protected by use of appropriate Information Security (INFOSEC) measures.
Information System	Assembly of equipment, methods and procedures and, if necessary, personnel organized to accomplish information processing functions. Note: An information system may also transfer information in support of the processing function, for example, over a local area network interconnecting a number of computers which are part of the information system. [Source: Defence Terminology Bank, Record 20171]
Information Technology	Includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation, and implementation of information systems and applications to meet business requirements. [Source: Treasury Board of Canada Secretariat, Policy Framework for Information and Technology, 1 July 2007]
Information Technology Asset	IT assets are any elements of software and/or hardware that are found in the Information Technology Infrastructure. [Information Management Group IM Standards, IMS 6002-9-1, 19 January 2012]
Information Technology Infrastructure	The set of computers, communications, systems software, utility programmes, and management tools which support the automation of information management throughout an organization.
Information Technology Security	Safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.
Information Technology Service	The discrete points of interaction between information technology and people, both internal and external to an organization.
Information Technology Systems	An assembly of computer hardware, software or firmware, either stand-alone or interconnected that is used to process or transmit data, or to control mechanical or other devices. [Source: Joint Terminology Panel, 2014]
Infrastructure as a service (IaaS)	Infrastructure as a service (IaaS) are online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. A hypervisor, such as Xen, Oracle VirtualBox, Oracle VM, KVM, VMware ESX/ESXi, or Hyper-V, LXD, runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. https://en.wikipedia.org/
Integrity	The state of being accurate, complete, authentic and intact.
Intelligence	The product resulting from the collection, processing, analysis, integration and interpretation of available information concerning foreign states, hostile or potentially hostile forces or elements, geography and social and cultural factors that contributed to the understanding of an actual or potential operating environment. **Note**: The term “intelligence” also applies to the activities that result in the product and to the organizations engaged in such activities. [DBT 738]

Term	Description
Multi-Tenant – Multi-tenancy	Multi-Tenant – Multi-tenancy means that a single instance of the software and its supporting infrastructure serves multiple customers. Each customer shares the software application and also shares a single database. Each tenant's data is isolated and remains invisible to other tenants. https://digitalguardian.com
On-premises	On-premises is the software and technology that is located within the physical confines of an enterprise often in the company's data center as opposed to running remotely on hosted servers or in the cloud. https://www.webopedia.com/
Operational Authority	means the person who has the authority to define requirements and operating principles, set standards and accept risk within there are of responsibility [DTB 43435]
Personnel Security	The application of security measures, in order to ensure that all personnel who have access to information have the required need-to-know and have the appropriate security clearance.
Physical Security	That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, documents and information, and to protect them against espionage, sabotage, terrorism, damage, and theft.
Programme	A set of related measures or activities with a particular long-term aim. [Oxford English Dictionary]
Project Information or Project Information and Assets	all documents (formal or drafts), correspondence, reports, presentations, meetings, discussions, descriptions, plans, requirements, financial data and budgets, concepts of operation, concepts of support, procurement plans and data, personnel resources, schedules, deliverables, specifications, system definitions, system configurations, system designs, software, hardware, system components and personnel created by, acquired for or otherwise working on behalf of the Project.
Provenance	means the beginning of something's existence; something's origin; a record of ownership of a work of art or an antique; used as a guide to authenticity or quality.
Risk management	Risk management, which involves a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on, and communicating risk issues, is an integral component of good management. It does not necessarily mean risk avoidance in the case of potential threats. Rather, risk management equips organizations to make decisions that are informed by an understanding of their risks, and ultimately to respond proactively to change by mitigating the threats, and capitalizing on the opportunities, that uncertainty presents to an organization's objectives. Sound risk management can lead to more effective, results-based, and high performance government. In turn, increased capacity and demonstrated ability to assess, communicate and respond to risks builds trust and confidence, both within the government and with the public. [Treasury Board of Canada Secretariat - Guide to Integrated Risk Management]
Risk Response	Refers to the continuum of measures of risk mitigation or control that are developed and implemented to address an identified risk.
Sensitive	means requiring special protection from disclosure that could cause embarrassment, threaten or compromise security e.g. Protected or classified information, assets or resources would be considered Sensitive.

Term	Description
Software as a service (SaaS)	Software as a service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software", and was formerly referred to as "software plus services" by Microsoft. SaaS applications are also known as Web-based software, on-demand software and hosted software. https://en.wikipedia.org/
Standard	Document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note: Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits. [DTB 44020]
Supply Chain (SC)	is the network of all the individuals, organizations, resources, activities and technology involved in the design, development, creation, packaging, transportation, delivery, installation, training, maintenance, disposal and ultimate operation of a System or Service, or parts thereof;
Supply Chain Compromise	means an occurrence within the supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. A supply chain compromise can occur anywhere within the system development life cycle of the product or service.
Supply Chain Integrity (SCI)	is the process of managing an organization's internal capabilities, as well as its partners and suppliers, to ensure all elements of an integrated solution are of high-assurance. It includes not just the supply chain of equipment, hardware and software but all the supply of Contracted Professional Services (personnel and support services) and organization personnel.
Technical Authority	means the person who has the authority to set technical specifications and standards, manage configurations, provide technical advice and monitor compliance within their area of responsibility. [DTB 43437]
Threat and Risk Assessment (TRA)	Threat and Risk Assessment (TRA) is a process for identifying assets and resources and assessing the level of risk to those assets and resources; evaluating threats, including the motivation, intent, capability of a threat agent and the opportunity, likelihood and consequence of threat acts that could place the delivery of critical services at risk; Examining and evaluating potential disruptions and events for the purpose of determining vulnerabilities and the implementation of countermeasures to reduce vulnerabilities. [DTB 43215]
Turnkey	**Adjective**: "of or involving the provision of a complete product or service that is ready for immediate use. "turnkey systems for telecommunications customers", Oxford

ANNEX "B"

Non Disclosure Agreement

I, _____ , recognize that in the course of my work as an employee or subcontractor of _____, I may be given access to information by or on behalf of Canada in connection with the Work, pursuant to Contract No. W6820-21ZZ02/A between Her Majesty the Queen in right of Canada, represented by the Minister of Public Works and Government Services and _____ , including any information that is confidential or proprietary to third parties, and information conceived, developed or produced by the Contractor as part of the Work. For the purposes of this agreement, information includes but not limited to: any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form, recorded electronically, or otherwise and whether or not labeled as proprietary or sensitive, that is disclosed to a person or that a person becomes aware of during the performance of the Contract.

I agree that I will not reproduce, copy, use, divulge, release or disclose, in whole or in part, in whatever way or form any information described above to any person other than a person employed by Canada on a need to know basis. I undertake to safeguard the same and take all necessary and appropriate measures, including those set out in any written or oral instructions issued by Canada, to prevent the disclosure of or access to such information in contravention of this agreement.

I also acknowledge that any information provided to the Contractor by or on behalf of Canada must be used solely for the purpose of the Contract and must remain the property of Canada or a third party, as the case may be.

I agree that the obligation of this agreement will survive the completion of the Contract Serial No.: W6820-21ZZ02/A.

_____

Signature

_____

Date

ANNEX "C"

SECURITY REQUIREMENTS CHECK LIST

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
W6820-21-ZZ02	
Security Classification / Classification de sécurité	
Unclassified	

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
National Defence	CFINTCOM

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

Establishment of a Supply Arrangement to provide IT solutions for the Defence Intelligence Enterprise.
See attached SRCL Supplemental and IT Security Requirements

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	✔ No / Non	Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	✔ No / Non	Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non	✔ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	✔ No / Non	Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	✔ No / Non	Yes / Oui

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

Canada ✔	NATO / OTAN ✔	Foreign / Étranger
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion	All NATO countries / Tous les pays de l'OTAN	No release restrictions / Aucune restriction relative à la diffusion
Not releasable / À ne pas diffuser ✔		
Restricted to: / Limité à :	Restricted to: / Limité à : ✔	Restricted to: / Limité à :
Specify country(ies): / Préciser le(s) pays : Canada	Specify country(ies): / Préciser le(s) pays : Canada	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)

PART A *(continued)* / PARTIE A *(suite)*

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

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

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

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

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

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

Special comments:
Commentaires spéciaux :

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRES SECRET
Information / Assets / Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
W6820-21-ZZ02	
Security Classification / Classification de sécurité	
Unclassified	

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Mr. Paul J. Morin	D Int IM	MORIN, PAUL 736 Digitally signed by MORIN, PAUL 736 Date: 2022.06.20 12:38:38 -04'00'	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613 945 5029		Paul.Morin@forces.gc.ca	Digitally signed by MORIN, PAUL 736 Date: 2022.02.24 11:04:31 -05'00'

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sasha Medjovic	Sr Security Analyst		
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613 996 0286		sasha.medjovic@forces.gc.ca	

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? ☐ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**

17. de sécurité

N	Titre	Signature	
T ieur		**E-mail address - Adresse courriel**	**Date**

Kelly Mureta
Contract Security Officer
Tel: 613-941-0441
kelly.mureta@tpsgc-pwgsc.gc.ca

ANNEX "D"

CONTRACT SECURITY PROGRAM APPLICATION FOR REGISTRATION (AFR)

CONTRACT SECURITY PROGRAM INITIAL INTERNATIONAL SECURITY SCREENING (IISS)

CONTRACT SECURITY PROGRAM (CSP)

APPLICATION FOR REGISTRATION (AFR) for Canadian legal entities

Instructions for completing the Application for Registration (AFR)

Privacy notice for Canadian entities registering in the CSP

Part of the information collected in this form includes personal information which is collected under the authority of subsection 7(1) of the *Financial Administration Act* and is mandatory in accordance with Treasury Board's *Policy on Government Security and Standard on Security Screening* for the purposes of security assessment and registration in the Contract Security Program (CSP) of Public Services and Procurement Canada (PSPC). The personal information will be used to assess your eligibility to hold a security status or security clearance and for your organization to be registered in the Contract Security Program. The information provided may be disclosed to the Royal Canadian Mounted Police and Canadian Security Intelligence Service to conduct the requisite checks and / or investigation in accordance with the Policy on *Government Security* and *Standard on Security Screening*. Additionally, the information may be disclosed to and used by other federal institutions that may require this information as part of their functions or investigation under Canadian Law or to the industrial security programs of foreign governments (with which Canada has bilateral security instruments) for foreign assurances.

Personal information is protected, used and disclosed in accordance with the Privacy Act and is described in the Info Source under the Personal Information Bank PWGSC PPU 015 (Access to information and privacy - PSPC (tpsgc-pwgsc.gc.ca) and the TBS standard personal information bank Personal Security Screening PSU 917 (Standard personal information banks - Canada.ca). Under the *Privacy Act*, you have the right to access and correct your personal information, if erroneous or incomplete. The personal information from paper sources that accompanies an organization registration is retained for two years after the last administrative action, and then destroyed. The personal information from paper sources that accompanies a foreign ownership, control, or influence assessments is kept for two years, and then destroyed if there are no changes to the organization that are reported to the foreign ownership, control, or influence evaluation office during this period. The personal information from paper sources that accompanies the personnel security screening process or foreign assurance process will be retained for a minimum period of two years after the last administrative action, and then destroyed. The Contract Security Program's retention period and disposal standards of personal information in electronic format may vary from the above retention period.

If you have concerns or require clarification about this privacy notice, you can contact PSPC's Access to Information and Privacy Directorate by email at TPSGC.ViePrivee-Privacy.PWGSC@tpsgc-pwgsc.gc.ca. If you are not satisfied with the response to your privacy concern or if you want to file a complaint about the handling of your personal information, you may wish to contact the Office of the Privacy Commissioner of Canada.

General Instructions:

- This form is used for registering Canadian legal entities **ONLY**. The CSP does not register foreign based organizations. **ALL** Foreign based firms must contact the International Industrial Security Directorate (IISD) for more information on the security screening process. Canadian subsidiaries of foreign based firms may be eligible to register with the CSP.
- This form and all supporting documentation requested must be provided in English or French
- In any instance where this form does not allow enough space for a complete answer, please include additional pages or rows to the table as required.

For organizations that do not yet have a clearance, refusal to provide required information, the provision of a false statement, misleading information, concealment or failure to disclose of any material fact on this application will result in the CSP not granting, or upgrading, a security clearance.

In the case of already cleared organizations; a denial or revocation of your organization's existing security clearance may occur and any personnel reliability statuses and/or personnel security clearances issued to your organization will be administratively closed out along with the organization's clearance with the Contract Security Program. This will immediately prohibit your eligibility to perform work on contracts requiring organization security clearances.

CONTRACT SECURITY PROGRAM (CSP)

Section A - Business Information

- **Legal name of the organization** refers to the legal name of the organization as it is organized & existing within the country of jurisdiction. In the case of Canadian legal entities, this would be the legal name that is registered with federal, provincial or territorial authorities.
- **Business or Trade name** refers to the name which a business trades under for commercial purposes, although its registered, legal name, used for contracts and other formal situations, may be another name.
- **Type of Organization** - All required documentation in relation to the type of organization must be provided
  - **Corporation** refers to an entity having authority under the law to act as a single person distinct from the shareholders who own it and having rights to issue stock and exist indefinitely.

    Provide the following information to substantiate this "Type of Organization" selection:
    - Stock exchange identifier (if applicable);
    - Certificate of incorporation, compliance, continuance, current articles of incorporation, etc.
    - Ownership structure chart is mandatory
  - **Partnership** refers to an association or relationship between two or more individuals, corporations, trusts, or partnerships that join together to carry on a trade or business.

    Provide the following information to substantiate this "Type of Organization" selection:
    - Evidence of legal status, ie. partnership agreement;
    - Provincial partnership name registration (if applicable);
    - Ownership structure chart
  - **Sole proprietor** refers to the owner of a business who acts alone and has no partners.

    Provide the provincial registration documentation (if applicable) ie. master business license, provincial name registration document
  - **Other** (universities, financial institutions, unincorporated organizations, Assembly of First Nations, etc.)

    Provide the following information to substantiate this "Type of Organization" selection:
    - Evidence of legal status such as acts, charters, bands, etc.
    - Ownership structure chart and management structure chart
- **Principal place of business** must be where the business is physically located and operating in Canada. Virtual locations, mail boxes, receiving offices, coworking spaces, representative agent's office, etc. will not be accepted.
- **Self-identify as a diverse supplier:** Public Services and Procurement Canada (PSPC) defines a diverse supplier as "a business owned or led by Canadians from underrepresented groups, such as women, Indigenous Peoples, persons with disabilities and visible minorities.

Section B - Security Officers

Identify the individual(s) you intend to nominate or are already appointed as your organization's company security officer and alternate company security officer(s). For Document Safeguarding Capability at other locations, please ensure to indicate address (site) the ACSO is located at. Add additional rows or provide a separate page as required. Employee has the same meaning as that used by the Canada Revenue Agency.

- Email address must be able to accept various types of correspondence from the CSP
- Security officers **must** meet all of the following criteria:
  - an employee of the organization;
  - physically located in Canada;
  - a Canadian citizen*; and
  - security screened at the same level as the organization (in some cases alternates may require a different level).

  *Canadian citizenship is required due to the oversight responsibility entrusted to a security officer and some contractual requirements in relation to national security. This requirement may be waived on a case by case basis for Permanent Residents.

CONTRACT SECURITY PROGRAM (CSP)

Section C - Officers

- Your organization must list **all** the names and position titles for its officers, management, leadership team, executives, managing partners, authorized signatories, members, etc. that are responsible for the day to day operations of its business. A management structure chart must be provided to demonstrate the reporting structure. Add additional rows to the section if required.
- For the purposes of the Contract Security Program, the term "Country of Primary Residence/National Domicile" refers to the particular country for a person's true, fixed, principal and permanent home, to which that person intends to return and remain even though currently residing elsewhere.
- **Citizenship** refers to the status of being a citizen. A **citizen** is a person who, by either birth or naturalization, is a member of a state or nation, entitled to enjoy all the civil rights and protections of that state or nation and owing allegiance to its government.

Section D - Board of Directors

- List **all** members of your organization's board of directors. Indicate all board titles including the chairperson if there is one. Add additional rows to the section or on a separate page if required.
- For the purposes of the Contract Security Program, the term "Country of Primary Residence/National Domicile" refers to the particular country for a person's true, fixed, principal and permanent home, to which that person intends to return and remain even though currently residing elsewhere.
- **Citizenship** refers to the status of being a citizen. A **citizen** is a person who, by either birth or naturalization, is a member of a state or nation, entitled to enjoy all the civil rights and protections of that state or nation and owing allegiance to its government.

Section E - Ownership Information

- For the purposes of the CSP, the following interpretations are applicable:
  - **Direct (or registered) ownership** are **all** owners who hold legal title to a property or asset in that owner's name.
  - **Ownership** refers to either (1) voting rights attached to the corporation's outstanding voting shares or (2) outstanding shares measured by fair market value.
  - **Parent company** refers to a company which owns and/or controls controlling interest (e.g., voting stock) of other firms or companies, usually known as subsidiaries, which may give it control of the operation of the subsidiaries.

Section F - Justification (this section is to be completed by organizations that are undergoing a renewal ONLY - not bidding)

- Your organization is to provide a list of active federal contracts, subcontracts, leases, supply arrangements (SA), standing offers (SO), purchase orders that have security requirements. Indicate the contract number (lease, SA, SO, sub-contract, etc.), contracting authority or prime contractor and the security level requirement.

Section G - Certification and Consent

- Only an officer identified in Section C may complete this section.

CONTRACT SECURITY PROGRAM (CSP)

APPLICATION FOR REGISTRATION (AFR) for Canadian legal entities

NOTE:
The provision of false, misleading information, or concealment and/or failure to disclose of any material fact on this application will result in a denial or revocation of your organization security clearance and registration with the Contract Security Program which will immediately prohibit your eligibility to perform on contracts requiring organization security clearances. An incomplete form **will not** be processed.

SECTION A - BUSINESS INFORMATION

1. Legal name of the organization

2. Business or trade name (if different from legal name)

3. Type of organization - **Indicate the type of organization and provide the required validation documentation (select one only)**

- ☐ Sole proprietor
- ☐ Partnership
- ☐ Corporation
  - ☐ Private
  - ☐ Public
- ☐ Other (specify)

4. Provide a brief description of your organization's general business activities.

5. Procurement Business Number (PBN) (if applicable)	6. Self-identify as a diverse supplier (provide profile)

7. Business civic address (head office)

8. Principal place of business (if not at head office)

9. Mailing address (if different from business civic address)

10. Organization website (if applicable)

11. Telephone number	12. Facsimile number
13. Number of employees in your organization or corporate entity	14. Number of employees requiring access to protected/ classified information/assets/sites

CONTRACT SECURITY PROGRAM (CSP)

SECTION B –SECURITY OFFICERS

Please identify all security officers for your organization. For document safeguarding capability identify the site number for each ACSO and the corresponding address for each site below.

Add additional rows or attachments as needed if there is not enough space allotted

Position title	Site #	Surname	Given name	E-mail (where the CSP will send correspondence)
Company security officer (CSO)				
Alternate company security officer (ACSO)				
ACSO (if applicable)				
ACSO (if applicable)				
ACSO (if applicable)				

For Document Safeguarding Capability ONLY:

00 – Address will be principal place of business	
01 – Site address:	
02 – Site address:	

SECTION C – OFFICERS (managing partners, key leadership, signatories, etc.)

Add additional rows or attachments as needed and include management structuree chart demonstrating reporting structures

Position title - within your organization	Surname	Given name	Citizenship(s)	Country of primary residence/National domicile

CONTRACT SECURITY PROGRAM (CSP)

SECTION D – LIST OF BOARD OF DIRECTORS

Add additional rows or attachments as needed

Position title	Surname	Given name	Citizenship(s)	Country of primary residence/National domicile

SECTION E - OWNERSHIP INFORMATION - PLEASE COMPLETE FOR EACH LEVEL OF OWNERSHIP

Please complete for each level of ownership

Identify all entities, individuals, public or private corporations that have an ownership stake in your organization being registered. Indicate if the entity has a valid Facility Security Clearance from Public Services and Procurement Canada's Contract Security Program or any other country. For publicly traded corporations, identify stock exchange. If there are more than three levels of ownership; please submit on an additional page to include **all** levels of ownership from direct to ultimate.

Note: The organization structure chart with percentages of ownership must be included with your submission

SECTION E-1 - OWNERSHIP LEVEL 1 (direct ownership) if more than three - please provide on additional sheet

Ownership - Level 1 (Direct Parent)			
Name of organization or individual			
Address			
Type of entity (e.g. private or public corporation, state-owned)			
Stock exchange identifier (if applicable)			
Facility security clearance (FSC) yes/no			
Percentage of ownership			
Country of jurisdiction or citizenship			

CONTRACT SECURITY PROGRAM (CSP)

SECTION E-2 - OWNERSHIP LEVEL 2

If there is any additional ownership for the names listed in the previous section (E-1) please provide the information below. If not, please indicate N/A (not applicable).

Ownership of entries listed in E-1 (Level 2)			
Name of direct owner from E-1			
Name of organization or individual			
Address			
Type of entity (e.g. private or public corporation, state-owned)			
Stock exchange identifier (if applicable)			
Facility security clearance (FSC) yes/no			
Percentage of ownership			
Country of jurisdiction or citizenship			

SECTION E-3 - OWNERSHIP LEVEL 3

If there is any additional ownership for the names listed in the previous section (E-2) please provide the information below. If not, please indicate N/A (not applicable).

Ownership of entries listed in E-2 (Level 3)			
Name of intermediary ownership from E-2			
Name of organization or individual			
Address			
Type of entity (e.g. private or public corporation, state-owned)			
Stock exchange identifier (if applicable)			
Facility security clearance (FSC) yes/no			
Percentage of ownership			
Country of jurisdiction or citizenship			

CONTRACT SECURITY PROGRAM (CSP)

SECTION F - JUSTIFICATION (FOR RENEWING ORGANIZATIONS)

Add additional rows or attachments as needed

Please provide all current procurement rationales that have security requirements - i.e. contracts, leases, RFP, RFI, ITQ, supply arrangements, standing offers, etc.

Contract, lease, SA, SO, etc. number	Client / contracting authority	Security Type & level	Expiry date (dd-mm-yyyy)

SECTION G - CERTIFICATION AND CONSENT (ONLY AN OFFICER IDENTIFIED IN SECTION C MAY COMPLETE THIS SECTION)

I, the undersigned, as the Officer authorized by the organization, have read the Privacy Notice to this application and do hereby certify that the information contained in this application is true, complete and correct. I acknowledge and agree to comply with the responsibilities outlined in the Public Services and Procurement Canada's Contract Security Manual and consent to the collection, use and disclosure of my personal information for the purposes as described above. **I agree to notify the Contract Security Program of any changes to the organization including but not limited to: change of address, phone number, contact information, change in security officers, officers and directors, board members, partners, management / leadership team and ownership.**

Surname	Given name
Position title	Telephone number (include extension number if any)
Facsimile number	Email address
Signature	Date (dd-mm-yyyy)

FOR USE BY THE PSPC'S CONTRACT SECURITY PROGRAM

Recommendations	
Recommended by e-signature	Approved by e-signature