National Defence
National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale
Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

REQUEST FOR A SUPPLY ARRANGEMENT / DEMANDE POUR UN ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT

RETURN OFFERS TO / RETOURNER LES OFFRES À:

TransportationContracting@forces.gc.ca

attn: Caroline Laflamme-Lafleur

Offer To: National Defence Canada
We hereby offer to provide to Canada, as represented by the Minister of National Defence, in accordance with the terms and conditions set out herein or attached hereto, the goods and/or services detailed herein and on any attached sheets.

Offre à : Défense nationale Canada
Nous offrons par la présente de fournir au Canada, représenté par le ministre de la Défense nationale, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens et/ou services énumérés ici et sur toute feuille ci-annexée.

Title / Titre:	**Solicitation No / No de l'invitation:**
Advisory and Consulting Services in support of the Defence Supply Chain (DSC) / Services de conseil et de consultation à l'appui de la chaîne d'approvisionnement de la Défense (CAD)	W6369-210242/A
Date of Solicitation / Date de l'invitation: 5 February 2021 / 5 février 2021	
Address Enquiries to – Adresser toutes questions à: TransportationContracting@forces.gc.ca attn: Caroline Laflamme-Lafleur	
Telephone No. / N° de téléphone: 613-297-6317	**FAX No / No de fax:** N/A
Destination: See herein - Voir ci-inclus	

Instructions:

Municipal taxes are not applicable. Unless otherwise specified herein all prices quoted must include all applicable Canadian customs duties, GST/HST, excise taxes and are to be delivered Delivery Duty Paid including all delivery charges to destination(s) as indicated. The amount of the Goods and Services Tax/Harmonized Sales Tax is to be shown as a separate item.

Instructions:

Les taxes municipales ne s'appliquent pas. Sauf indication contraire, les prix indiqués doivent comprendre les droits de douane canadiens, la TPS/TVH et la taxe d'accise. Les biens doivent être livrés «rendu droits acquittés», tous frais de livraison compris, à la ou aux destinations indiquées. Le montant de la taxe sur les produits et services/taxe de vente

Solicitation Closes / L'invitation prend fin:

At / à : 14:00 Eastern Standard Time (EST) / 14:00 heure normal de l'est (HNE)

On / le : 2 March 2021 / 2 mars 2021

Delivery required / Livraison exigée:	**Delivery offered / Livraison proposée:**
See herein - Voir ci-inclus	

Vendor Name and Address / Raison sociale et adresse du fournisseur:

Name and title of person authorized to sign on behalf of vendor (type or print) / Nom et titre de la personne autorisée à signer au nom du fournisseur (caractère d'imprimerie):

Name / Nom: _____ **Title / Titre: _____**

Signature:_____ **Date: _____**

Canada

NOTICE TO BIDDERS

A supply arrangement is a method of supply used by the Department of National Defence (DND) to procure goods and services. A supply arrangement is an arrangement between Canada and pre-qualified suppliers that allows identified users to solicit bids from a pool of pre-qualified suppliers for specific requirements within the scope of a supply arrangement. A supply arrangement is not a contract for the provision of the goods and services described in it and neither party is legally bound as a result of signing a supply arrangement alone. The intent of a supply arrangement is to establish a framework to permit expeditious processing of individual bid solicitations which result in legally binding contracts for the goods and services described in those bid solicitations.

Except for those procurements where public advertising is not required or used, Requests for Supply Arrangements (RFSA) are posted on the Government Electronic Tendering Service (GETS) and suppliers who are interested in responding to individual bid solicitations issued under a supply arrangement framework are invited to submit an arrangement to become pre-qualified suppliers. The list of pre-qualified suppliers will be used as a source list for procurement within the scope of the supply arrangement and only suppliers who are pre-qualified at the time individual bid solicitations are issued will be eligible to bid. Supply arrangements include a set of predetermined conditions that will apply to subsequent bid solicitations and contracts. Supply arrangements may include ceiling prices which may be lowered based on an actual requirement or scope of work described in a bid solicitation.

TABLE OF CONTENTS

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 Security Requirement Check List.

1.2 Summary

1.2.1 The objective of this Request for Supply Arrangement (RFSA) is to establish a list of pre-qualified firms capable of providing the Department of National Defense (DND) with a broad range of advisory and consulting services in Supply Chain Management. The list of pre-qualified suppliers will be used as a source list for various requirements to support the Defence Supply Chain (DSC) Governance authorities in their decision making and oversight roles.

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 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;
   (b) the Supplier's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 6A - Supply Arrangement;
   (c) the Supplier must provide the addresses of proposed sites or premises of work performance and document safeguarding as indicated in Part 3 - Section Ill Additional Information.

2. Suppliers are reminded to obtain the required security clearance promptly. Any delay in the issuance of a supply arrangement to allow the successful Supplier to obtain the required clearance will be at the entire discretion of the Supply Arrangement Authority.

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.

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 **(**2020-05-28) Standard Instructions - Request for Supply Arrangements - Goods or Services, are incorporated by reference into and form part of the RFSA, with the following modifications:

a) Section 02 Procurement Business Number is deleted in its entirety.

b) Section 05 Submission of arrangements: Subsection 5.4 of 2008, Standard Instructions - Request for Supply Arrangements - Goods or Services, is amended as follows:

Delete: 60 days
Insert: 90 days

2.2 Submission of Arrangements

Unless specified otherwise in the RFSA or otherwise directed by the Supply Arrangement Authority (SAA), arrangements must be submitted to the Department of National Defence organization by electronic mail by the date and time indicated on page 1 of the solicitation.

Individual e-mails that may include certain scripts, formats, embedded macros and/or links, or those that exceed five (5) megabytes may be rejected by Canada's e-mail system and/or firewall(s) without notice to the Supplier or Supply Arrangement Authority. Larger arrangements may be submitted through more than one e-mail. Canada will confirm receipt of documents. It is the Supplier's responsibility to ensure that their entire arrangement has been received. Suppliers should not assume that all documents have been received unless Canada confirms receipt of each document. In order to minimize the potential for technical issues, suppliers are requested to allow sufficient time before the closing date and time to confirm receipt. Arrangement documents submitted after the closing time and date will not be accepted.

Due to the nature of the Request for Supply Arrangements, transmission of arrangements by facsimile or via epost Connect service 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 five (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

The arrangement must be gathered per section and separated as follows:

Section I: Technical Arrangement
Section II: Certifications
Section III: Additional Information

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.

Section III: Additional Information

3.1.1 Supplier's Proposed Sites or Premises Requiring Safeguarding Measures

3.1.1.1 As indicated in Part 1 under Security Requirements, the Supplier must provide the full addresses of the Supplier's and proposed individuals' sites or premises for which safeguarding measures are required for Work Performance. Storage, processing, and/or creation of government sensitive (Designated or Classified) information outside of Canada is not authorized under this supply arrangement.

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory
Postal Code
Canada

3.1.1.2 The Company Security Officer must ensure through the Contract Security Program that the Supplier and proposed individual(s) hold a valid security clearance at the required level, as indicated in Part 1, clause 1.3, Security Requirements.

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 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

Mandatory Technical Criteria are included in Attachment 1 to Part 4.

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.

ATTACHMENT 1 TO PART 4 – MANDATORY TECHNICAL CRITERIA

a) The technical arrangement must meet the mandatory technical criteria specified below. The Supplier must provide the necessary documentation to support compliance with this requirement.

b) Arrangements which fail to meet the mandatory technical criteria will be declared non-responsive. Each mandatory technical criterion should be addressed separately.

c) If requested by Canada during the evaluation period, the Supplier must provide customer references within three (3) business days of a request by the Supply Arrangement Authority. The reference must be able to validate the facts identified in the Supplier's proposal. If additional time is required by the Supplier, the Supply Arrangement Authority may grant an extension in his or her sole discretion. If references are part of mandatory technical criteria, failure to provide this information within the timeframe stipulated will render the arrangement non-responsive. If there is a conflict between the information provided by the customer reference and the arrangement, the information provided by the customer reference will be evaluated instead of the information in the arrangement.

d) Definitions:

Supplier: as per SACC 2008 **(**2020-05-28) Standard Instructions - Request for Supply Arrangements - Goods or Services, "Supplier" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting an arrangement. It does not include the parent, subsidiaries or other affiliates of the Supplier, or its subcontractors.

	MANDATORY TECHNICAL CRITERIA & ARRANGEMENT PREPARATION INSTRUCTIONS	CROSS REFERENCE WITH ARRANGEMENT
MT1	The Supplier must have experience in all of the following three (3) types of supply chain management consulting services, which are based on Section 4.1 of Annex A, Statement of Work: A. Strategic Supply Chain Management Consulting Services, which could include activities such as: a. Advising on, reviewing and/or producing strategies and implementation plans in support of the overall supply chain strategy; b. Advising on, reviewing and/or producing the supply chain performance metrics, dashboards and benchmarks; c. Advising on, reviewing and/or producing a supply chain costing model for Return on Investment decision making; d. Advising on, reviewing and/or producing strategies and implementation plans in support of the supply chain resilience; e. Advising on, reviewing and/or producing strategies and implementation plans in support of the supply chain Sustainability; f. Advising on, reviewing and/or producing strategies and implementation plans in support of the supply chain Program Management; g. Advising on, reviewing and/or producing strategies and implementation plans in support of the supply chain Change Management. B. Technological Supply Chain Management Consulting Services, which could include activities such as: a. Advising on, and/or reviewing the supply chain technology currently in use from strategic, operational and tactical levels of operations; b. Advising on, and/or reviewing the exploitation of an Enterprise Resource Planning (ERP) solution such as SAP and its ability to plan a task force structure; c. Advising on, reviewing, and/or producing feasibility studies or implementation of a Supply Chain Event Management System; d. Advising on, reviewing, and/or producing a digital supply chain strategy. C. Supply Chain Management Processes Consulting Services, which could include activities such as: a. Advising on, reviewing, and/or implementing Lean Six Sigma program; b. Advising on, reviewing, and/or implementing business process reengineering; c. Advising on, reviewing, and/or implementing a supply chain Process Optimization; d. Advising on, reviewing, and/or implementing a supply chain process and operational training. The Supplier must provide a total of three (3) project references. Each project reference must address at least one (1) of the three (3) types of supply chain management consulting services listed above. Experience in all three (3) must be demonstrated amongst the referenced projects. For example, Project 1 could demonstrate experience in A., Project 2 experience in both A. and C., and Project 3 experience in B.. The list of activities included above are provided for reference. The Supplier does not have to demonstrate experience in all the listed activities in order to be compliant. The referenced projects must meet the eligibility criteria listed below: I. The project must be for an organization operating a complex multi-echelon supply chain across a national geographically disparate environment of at least five (5) different provinces, states, or countries, which includes multiple distribution centres, and incorporate at least two (2) different commodity types (e.g. food, spare parts, equipment, fuel, etc.). II. The contract value of the project must have exceeded $200,000 CAD including taxes. III. The project must have achieved measurable results, including but not limited to cost savings, and performance improvements. IV. The project must have been performed within the last five (5) years from the closing date of RFSA W6369-210242/A. Projects currently underway are acceptable, as long as demonstrable results have already been obtained. V. At least one project must have included the use of supply chain simulation and modelling software to design and implement solutions. VI. At least one project must demonstrate end to end capabilities by including implementation of the changes to the supply chain (i.e. the Supplier must have been involved in the implementation phase). For each project, the Supplier must provide the information requested in table MT1 below. A maximum of 3 projects will be evaluated. If more than 3 projects are submitted, only the first 3 in order of presentation will be evaluated.	To be completed by the Supplier (reference to section of the arrangement).

	MANDATORY TECHNICAL CRITERIA & ARRANGEMENT PREPARATION INSTRUCTIONS	CROSS REFERENCE WITH ARRANGEMENT
MT2	The Supplier must have experience providing Consulting Services that are Specific to at least four (4) of the following six (6) Supply Chain Management Business Activities, which are based on Section 3.2 of Annex A, Statement of Work: 1. Plan 2. Acquisition 3. Distribution 4. Warehousing 5. Support 6. Divestment The Supplier must provide two (2) project references. Each project reference must address at least three (3) of the six (6) Supply Chain Management Business Activities listed above. Experience in at least four (4) Supply Chain Management Business Activities must be demonstrated amongst the referenced projects. For example, Project 1 could demonstrate experience in 1., 2. and 4., and Project 2 experience in 1. 2., 4. and 5. The referenced projects must meet the eligibility criteria listed below: I. The project must be for an organization operating a complex multi-echelon supply chain across a national geographically disparate environment of at least five (5) different provinces, states, or countries, which includes multiple distribution centres, and incorporate at least two (2) different commodity types (e.g. food, spare parts, equipment, fuel, etc.). II. The contract value of the project must have exceeded $200,000 CAD including taxes. III. The project must have achieved measurable results, including but not limited to cost savings, and performance improvements. IV. The project must have been performed within the last five (5) years from the closing date of RFSA W6369-210242/A. Projects currently underway are acceptable, as long as demonstrable results have already been obtained. V. At least one project must have included the use of supply chain simulation and modelling software to design and implement solutions. For each project, the Supplier must provide the information requested in table MT2 below. A maximum of 2 projects will be evaluated. If more than 2 projects are submitted, only the first 2 in order of presentation will be evaluated.	To be completed by the Supplier (reference to section of the arrangement).
MT3	The Supplier must provide a Corporate Profile and Human Resources Plan demonstrating that it has the capacity to provide consulting and advisory services in support of the Defence Supply Chain (DSC) Management, as described in the Statement of Work. At a minimum, the following elements must be addressed: **1. Corporate Profile:** 1.1. Overview of the Supplier's existing workforce specialized in the supply chain domain. 1.2. Brief description of the Supplier's established quality assurance framework. 1.3. Brief description of the tools and software that are available to the Supplier to support activities such as data analytics, modeling, optimization, cost analysis, etc. **2. Human Resources Plan:** 2.1. Supplier's ability to provide expertise in a variety of fields in a timely manner. For example, expertise in supply chain management, change management, cost and risks management, data analytics, etc. 2.2. Supplier's ability to support multiple requirements simultaneously. The Corporate Profile and Human Resources Plan should not exceed 8 pages in total (i.e. maximum of 8 pages for criterion MT3). Information contained in pages in excess of 8 pages will not be evaluated. Pages should be in Letter size (8.5 x 11 inch) and font should be no smaller than 10 points.	To be completed by the Supplier (reference to section of the arrangement).

Suppliers must provide the following information for each project referenced in MT1. Suppliers should provide their response using the following template:

TABLE MT1	
Project #	
Project Name	
Client Organization	
Supply Chain Complexity	
Contract Value (CAD)	$
Period	From: To:
Project Summary	
Project measurable results	
Types of Supply Chain Management Consulting Services	**The Supplier must demonstrate how the experience gained is relevant to the Type(s) of Supply Chain Management Consulting Services.**
A. Strategic Supply Chain Management Consulting Services	
B. Technological Supply Chain Management Consulting Services	
C. Supply Chain Management Processes Consulting Services	
Additional Eligibility Criteria (if applicable)	**The Supplier must demonstrate how the experience gained meets the additional eligibility criteria, if applicable.**
Supply chain simulation and modelling software to design and implement solutions.	
End to end capabilities by including implementation of the changes to the supply chain.	

Suppliers must provide the following information for each project referenced in MT2. Suppliers should provide their response using the following template:

TABLE MT2	
Project #	
Project Name	
Client Organization	
Supply Chain Complexity	
Contract Value (CAD)	$
Period	From: To:
Project Summary	

Project measurable results	
Types of Supply Chain Management Consulting Services	**The Supplier must demonstrate how the experience gained is relevant to the Supply Chain Management Business Activities.**
D. Consulting Services that are Specific to the following six (6) Supply Chain Management Business Activities: 1. Plan 2. Acquisition 3. Distribution 4. Warehousing 5. Support 6. Divestment	
Additional Eligibility Criteria (if applicable)	**The Supplier must demonstrate how the experience gained meets the additional eligibility criteria, if applicable.**
Supply chain simulation and modelling software to design and implement solutions.	

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.

All suppliers, regardless of their status under the policy, must submit the following information when participating in a procurement process or real property transaction:

- Suppliers that are corporate entities, including those bidding as joint ventures, must provide a complete list of the names of all current directors or, for a privately owned corporation, the names of the owners of the corporation;
- Suppliers bidding as sole proprietors, including sole proprietors bidding as joint ventures, must provide a complete list of the names of all owners;
- Suppliers that are a partnership do not need to provide a list of names.

Name of Supplier: _____

Name of each member of the joint venture:
Member 1: _____
Member 2: _____

Identification of the directors / owners:

NAME	FIRST NAME	TITLE

5.2.2 Additional Certifications Precedent to Issuance of a Supply Arrangement

5.2.2.2 Education and Experience

5.2.2.2.1 *SACC Manual* clause S1010T (2008-12-12) Education and Experience

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 – Canadian Suppliers

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.

6.2.1.1 The Contractor/Offeror must, at all times during the performance of the Contract/supply arrangement, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

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

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

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

6.2.1.5 The Contractor/Offeror must comply with the provisions of the:

(a) Security Requirements Check List and security guides, attached at Annex B;
(b) *Contract Security Manual* (Latest Edition)

6.2.2 Supplier's Sites or Premises Requiring Safeguarding Measures

6.2.2.1 Where safeguarding measures are required in the performance of the Work, the Supplier must diligently maintain up-to-date the information related to the Supplier's and proposed individuals' sites or premises, for the following addresses. Storage, processing, and/or creation of government sensitive (Designated or Classified) information outside of Canada is not authorized under this supply arrangement.

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory
Postal Code
Canada

6.2.2.2 The Company Security Officer must ensure through the Contract Security Program that the Contractor and individual(s) hold a valid security clearance at the required level.

6.3 Security Requirements – Foreign Suppliers

6.3.1 The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority for confirming **Contractor/Offeror** compliance with the security requirements for foreign suppliers.

6.3.2 The following security requirements apply to the foreign recipient **Contractor/Offeror** incorporated or authorized to do business in a jurisdiction other than Canada and delivering outside of Canada the services listed and described in the subsequent **contract/supply arrangement**.

6.3.2.1 The Foreign recipient **Contractor/Offeror** must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

6.3.2.2 The Foreign recipient **Contractor/Offeror** must, at all times during the performance of the **contract/supply arrangement**, hold an equivalence to a valid Designated Organization Screening (DOS), issued by the Canadian DSA as follows:

i. The Foreign recipient **Contractor/Offeror** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

ii. The Foreign recipient **Contractor/Offeror** must not begin the work, services or performance until the Canadian DSA is satisfied that all contract security requirement conditions have been met. Canadian DSA confirmation must be provided, in writing, to the foreign recipient **Contractor** in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.

iii. The Foreign recipient **Contractor/Offeror** must identify an authorized Contract Security Officer (CSO) and an Alternate (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in the **contract**. This individual will be appointed by the proponent foreign recipient **Contractor/Offeror's** Chief Executive Officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the contract.

iv. The Foreign recipient **Contractor/Offeror** must not grant access to **CANADA PROTECTED A or B** information/assets, except to its personnel subject to the following conditions:

   a. Personnel have a need-to-know for the performance of the **contract/supply arrangement**;

   b. Personnel have been subject to a Criminal Record Check, with favourable results, from a recognized governmental agency or private sector organization in **their country** as well as a Background Verification, validated by the Canadian DSA.

   c. The Foreign recipient **Contractor** must ensure that personnel provide consent to share results of the Criminal Record Check(s) with the Canadian DSA and other Canadian Government Officials, if requested; and

   d. The Government of Canada reserves the right to deny access to **CANADA PROTECTED** information/assets to a foreign recipient **Contractor/Offeror** for cause.

6.3.2.3 **CANADA PROTECTED** information/assets provided or generated pursuant to this **contract/supply arrangement** must not be further provided to a third party Foreign recipient Subcontractor unless:

a. written assurance is obtained from the Canadian DSA to the effect that the third-party Foreign recipient Subcontractor has been approved for access to **CANADA PROTECTED** information/assets by the Canadian DSA; and
b. written consent is obtained from the Canadian DSA, if the third-party Foreign recipient Subcontractor is located in a third country.

6.3.2.4 The Foreign recipient **Contractor/Offeror** MUST NOT remove **CANADA PROTECTED** information/assets from the identified work site(s), and the foreign recipient **Contractor/Offeror** must ensure that its personnel are made aware of and comply with this restriction.

6.3.2.5 The Foreign recipient **Contractor/Offeror** must not use the **CANADA PROTECTED** information/assets for any purpose other than for the performance of the **contract/subcontract/supply arrangement** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

6.3.2.6 The Foreign recipient **Contractor/Offeror** must, at all times during the performance of the **contract/subcontract/supply arrangement** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED B**.

6.3.2.7 All **CANADA PROTECTED** information/assets, furnished to the foreign recipient **Contractor/Offeror** or produced by the foreign recipient **Contractor/Offeror**, must also be safeguarded as follows:

a. Storage, processing, and/or creation of **CANADA PROTECTED** information outside of Canada is not authorized under this **contract/supply arrangement**.
b. The Foreign recipient **Contractor/Offeror** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/ assets pursuant to this **contract/supply arrangement** has been compromised.
c. The Foreign recipient **Contractor/Offeror** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/ assets accessed by the foreign recipient **Contractor/Offeror**, pursuant to this **contract/supply arrangement**, have been lost or disclosed to unauthorized persons.
d. The Foreign recipient **Contractor/Offeror** must not disclose **CANADA PROTECTED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent must be sought through the Canadian DSA.
e. The Foreign recipient **Contractor/Offeror** must provide the **CANADA PROTECTED** information/assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.
f. Upon completion of the Work, the foreign recipient **Contractor/Offeror** must return to the Government of Canada, all **CANADA PROTECTED** information/assets furnished or produced pursuant to this **contract**, including all **CANADA PROTECTED** information/assets released to and/or produced by its subcontractors.
g. The foreign recipient **Contractor/Offeror** requiring access to **CANADA PROTECTED A or B** information/ assets, under this **contract/supply arrangement**, must submit a Request for Site Access to the Chief Security Officer of **Department of National Defence**.

h. The Foreign recipient **Contractor/Offeror** MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system any **CANADA PROTECTED A or B** information/assets until authorization to do so has been confirmed by the Canadian DSA.
i. See Annex B Security Requirements Check List for security measures required for the treatment and access to **CANADA PROTECTED A or B** information.

6.3.2.8 In the event that a foreign recipient **Contractor/Offeror** is chosen as a supplier for this **contract/supply arrangement**, subsequent country-specific foreign security requirement clauses must be generated and promulgated by the Canadian DSA, and provided to the Contracting Authority/Supply Arrangement Authority, to ensure compliance with the security provisions, as defined by the Canadian DSA, in relation to equivalencies.

6.3.2.9 Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of the Canadian DSA.

6.3.2.10 All Subcontracts awarded to a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

6.3.2.11 All Subcontracts awarded by a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

6.3.2.12 The Foreign recipient **Contractor/Offeror** must comply with the provisions of the Security Requirements Check List attached at Annex B.

6.3.2.13 Canada has the right to reject any request to electronically access, process, produce, transmit or store **CANADA PROTECTED** information/assets related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

6.4 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.

6.4.1 General Conditions

2020 (2020-07-01) General Conditions - Supply Arrangement - Goods or Services, apply to and form part of the Supply Arrangement.

6.5 Term of Supply Arrangement

6.5.1 Period of the Supply Arrangement

The Supply Arrangement has no defined end-date and will remain valid until such time as Canada no longer considers it to be advantageous to use it.

The period for awarding contracts under the Supply Arrangement begins *(insert at award).*

6.5.2 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.

6.6 Authorities

6.6.1 Supply Arrangement Authority

The Supply Arrangement Authority is:

Name: Caroline Laflamme-Lafleur
Title: Senior Procurement Officer
Department of National Defence
ADM (Mat) / DG Proc Svcs / D Maj Proc 8
Mailing Address: 101 Col By Drive, Ottawa, ON K1A 0K2

Telephone: 613-297-6317
E-mail address: caroline.laflamme-lafleur@forces.gc.ca

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

6.6.2 Supplier's Representative

(insert at award)

6.7 Identified Users

The Identified User is the Department of National Defence.

6.8 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.

6.9 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 (2020-07-01), General Conditions - Supply Arrangement - Goods or Services
(c) Annex A, Statement of Work
(d) Annex B, Security Requirements Check List

(e) the Supplier's arrangement dated _____ (*insert date of arrangement*) *(if the arrangement was clarified or amended, insert at the time of issuance of the arrangement:* "as clarified on _____" ***or*** "as amended _____"*. (Insert date(s) of clarification(s) or amendment(s), if applicable)*.

6.10 Certifications and Additional Information

6.10.1 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.

6.11 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 Ontario.

B. BID SOLICITATION

6.1 Bid Solicitation Documents

Canada will use the following bid solicitation template:

- High Complexity (HC).

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

Note: References to the HC template is provided as an example only. The latest version 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;

(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 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*.*

(h) 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.

6.2.3 The bid solicitation will be issued by the Supply Arrangement Authority.

6.2.4 Thresholds and timelines:

Requirements estimated at $40,000.00 or less, taxes included
DND may direct the requirement to a specific SA Holder or invite SA Holders to respond within 5 calendar days from the bid solicitation date.

Requirements exceeding $40,000.00, taxes included
All SA Holders are invited to respond within 10-15 calendar days from the bid solicitation date.

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:

HC (for high complexity requirements), general conditions 2035 will apply to the resulting contract.

A copy of the template 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 template in Requests for Supply Arrangements is provided as an example only. The latest versions of the template and terms and conditions will be used at time of bid solicitation.

6.2 Supplemental

Due to the nature of the work, possible interdependencies and follow-on work, DND anticipates that any intellectual property rights arising from the performance of the work under any resulting contract will belong to Canada, on the ground that the Foreground IP consists of material subject to copyright.

For contracts to be awarded using the **HC** template, Supplemental General Condition 4007 Canada to Own Intellectual Property Rights in Foreground Information will apply.

Additional Supplemental conditions might apply to resulting contracts.

ANNEX A, STATEMENT OF WORK

1. Title

Advisory and Consulting Services in support of the Defence Supply Chain (DSC)

2. Objective

The objective of this Request for Supply Arrangement (RFSA) is to establish a list of pre-qualified firms capable of providing the Department of National Defense (DND) with a broad range of services and expertise in Supply Chain Management. The list of pre-qualified suppliers will be used as a source list for various requirements to support the DSC Governance authorities in their decision making and oversight roles.

3. Background

3.1. Defence Supply Chain Overview

The Department of National Defence Supply Chain exists to ensure the delivery of materiel required by the Canadian Armed Forces (CAF) is optimized to enable the CAF to execute its assigned Defence Tasks.

The Department of National Defence maintains and manages Inventories and Tangible Capital Assets (including Machinery and Equipment, Ships, Aircraft and Vehicles, Leased Tangible Capital Assets and Work in Progress) with a current book value of approximately $75B, within this number are inventories accounting for $6.2B.

The DSC comprises over 600 million items spanning roughly 1.2M NATO Stock Numbers (NSNs), globally dispersed across more than 300 supply warehouses with 6.1 million+ cubic meters of space, as well as at various private sector suppliers. Sound management of the planning, acquisition, support, warehousing, distribution and disposal of materiel is required to deliver against CAF operational needs while meeting departmental stewardship obligations in an effective manner.

The DSC is complicated and spans a number of organizations and departments with a depth and breadth of inventory rivalling the largest in industry. It is a strategic asset that supports defence operations in Canada and abroad, and its complex business processes comprise all activities from materiel acquisition, storage, distribution, maintenance and disposal.

The DSC manages the vital flow of materiel from commercial suppliers and back, in the case of repairable items, through a complex network of storage, distribution, and maintenance facilities that provide 1st Line operational units with the defence materiel they need to successfully conduct operations in Canada or abroad. Depending on the chosen materiel management and distribution strategy, this materiel may flow directly to and from the 1st Line units, or be routed through 3rd Line Military Supply depots, and/or 2nd Line local bases /area support units. In case of bulk or life time buys, some materiel will remain stored in DND’s warehouse space until it is needed for operations. For the purposes of this document, the lines of supply are described as follows:

a. First Line: A ship, battalion, squadron, base section or equivalent size unit is a first line organization with first line supply locations. Based on its role, the unit is provided with appropriate equipment and inventory to employ or operate;
b. Second Line: The materiel storage locations in a supply ship, service battalion, air maintenance squadron, base, wing or unit that primarily provides technical and materiel support to other units, or other parts of the base. Second line organizations may draw on the

resources of third line organizations to replenish their stocks or to supplement their resources; and

c. Third Line: There are eight third line supply locations, four of which are dedicated to ammunition and explosives. These locations are used for longer term storage or where it is impractical to pre-position materiel at every point of use. Over 67% of inventory, by value, is held at these third line locations at any given moment.

Unlike commercial supply chains and organizations that can often accept being out of stock of certain items, DND must always be provisioned to succeed on operations. The DSC must always have sufficient critical spare parts and other defence materiel readily available and positioned appropriately to meet mission requirements. Conversely, DND must exercise sound stewardship of its resources. It cannot afford to buy excess stock and/or create duplicate materiel requests because materiel appears to be lost in-transit between operations, DND organizations, or commercial repair facilities. It has the added challenge of information security to protect the integrity of ongoing global operations.

3.2. Defence Supply Chain Business Activities

The principle interconnected business activities of the DSC are as follows:

1. Plan: Identification, prioritization, and measuring of defence materiel requirements that ensure optimized realization of the CAF operational needs and accountability obligations within assigned resources (examples: right sized inventories, effective materiel positioning).

2. Acquisition: Sourcing, procurement and contracting methods to acquire defence materiel and services.

3. Distribution: Movement of materiel throughout the supply chain from supplier to user and all points in between and back again for repair or disposal.

4. Warehousing: Storage of defence materiel throughout the supply chain from supplier to user, in an efficient manner that complies with operational security legislation and regulatory guidelines (examples: hazardous materiel, controlled goods).

5. Support: Engineering and maintenance (In-Service Support) necessary to sustain materiel at prescribed readiness and materiel assurance levels.

6. Divestment: Removal from defence inventory, in accordance with applicable legislation, policy and approved disposal methods, materiel and equipment that is no longer required by the CAF, or to reduce existing inventory levels as required, in a cost effective manner.

3.3. Defence Supply Chain Management

Joint accountability for the effective management of the DSC has been assigned to Assistant Deputy Minister (Materiel) (ADM(Mat)) and Director of Staff Strategic Joint Staff (DOS SJS). The governance structure is represented as follow:

a. Defence Supply Chain Oversight Committee: Govern, oversee, and manage the Defence Supply Chain between DND and the Canadian Armed Forces.

b. Defence Supply Chain Steering Committee: Enable and monitor the execution of improvements to DSC performance. This committee has decision authority and will report to the Defence Supply Chain Oversight Committee.

c. Defence Supply Chain Planning and Operational Committee: Oversee implementation and delivery of Defence Supply Chain initiatives, the Management Action Plans resulting from independent audits and addressing integration issues across the Defence Supply Chain.

3.4. Defence Supply Chain Strategic Objectives

The key strategic objectives of the DSC reflect major and distinct lines of effort with measurable outcomes. These objectives drive activity to improve DSC performance and align to departmental strategic objectives. The DSC strategic objectives are as follows:

a. Right Sized Inventory: Optimized inventory holdings, accurately reflected in the Department's systems of record that meet operational materiel requirements of the CAF aligned with the CAF's force posture and readiness objectives and Government expectations on materiel management against a whole of DSC cost impacts through sound materiel planning, forecasting and supply management discipline.

b. Optimized Distribution: A distribution system that delivers effective and efficient service against prescribed service standards.

c. Acceptable Resilience: Level of agility founded on a comprehensive understanding of materiel holdings, implicating factors across in-service contracts and suppliers with vulnerabilities in individual critical asset supply chains understood and mitigated to an acceptable level of risk to enable surge of materiel support commensurate with Defence Policy's concurrency of operations objective.

d. Precise End-to-End DSC Planning: Comprehensive planning across DSC activities and affected Level 1 organizations to deliver continually optimized supply chain performance. This includes integrating "support" activity planning as well as visibility and expenditure with downstream supply chain to ensure that inventory levels are appropriate and neither at excess or at critically low levels. This includes consideration and alignment of maintenance program rationalizations and innovative in service support strategies.

e. Synchronized Transformation: Pan-Level 1 DSC business requirements are integrated and sequences across DSC practitioners and function enablers such as Enterprise Resource Planning functionality, analytics, professionalization and infrastructure. This objective also includes integrating and monitoring DSC input into several DND DSC initiatives.

f. Optimized Cost: The total cost to serve across the DSC has been defined and known, and DND continuously improves DSC efficiencies in support delivery through full understanding and judicious management of cost drivers.

g. DSC Professionalization: The DSC practitioners receive appropriate and standardized training, are enabled with technology and modernized processes, and are diligent in the disciplined execution of tasks necessary to respect both compliance with departmental and Treasury Board policy and operational requirements of the CAF.

3.5. Applicable Documents

References:

3.5.1. Strong, Secure, Engaged. Canada's Defence Policy, November 2017. (https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html)

3.5.2. Supply Administration Manual (SAM)

3.5.3. Procurement Administration Manual (PAM)

3.5.4. Report 3 - Supplying the Canadian Armed Forces, Auditor General of Canada, Spring 2020 (https://www.oag-bvg.gc.ca/internet/English/parl_oag_202007_03_e_43574.html)

4. Scope of Work

DND will require consulting services to support DSC governance authorities in their decision making and oversight roles in order to ensure the DSC Strategic Objectives are achieved.

The Supplier may be requested to collect and/or review information, conduct analysis and research and, where appropriate, provide actual strategies, action plans and other recommendations to improve or effect change in the Defence Supply Chain.

Below are examples of requirements which may be contracted for under the SA. This list is not meant to be firm nor exhaustive, but illustrative in nature of the range and type of tasks, activities, and deliverables that could be required.

The exact scope, tasks and deliverables will be defined in each requirement.

4.1. Tasks (examples)

4.1.1. **Strategic**

a. Advising on, reviewing and/or producing strategies and implementation plans in support of the overall DSC strategy ;
b. Advising on, reviewing, and/or producing DSC performance metrics, dashboards and benchmarks;
c. Advising on, reviewing and/or producing DSC costing models for Return on Investment decision making;
d. Advising on, reviewing and/or producing strategies and implementation plans in support of DSC resilience;
e. Advising on, reviewing and/or producing strategies and implementation plans in support of DSC Sustainability;
f. Advising on, reviewing and/or producing strategies and implementation plans in support of DSC Program Management;
g. Advising on, reviewing and/or producing strategies and implementation plans in support of DSC Change Management.

4.1.2. **Technological**

a. Advising on, and/or reviewing existing DSC technology currently in use from strategic, operational and tactical levels of operations;
b. Advising on, and or reviewing the exploitation of the existing SAP Enterprise Resource Planning (ERP) and its ability to plan a task force structure;
c. Advising on, reviewing and/or producing feasibility studies or implementation of a Supply Chain Event Management System;
d. Advising on, reviewing, and/or producing the digital Supply Chain strategy.

4.1.3. **Process Oriented**

a. Advising on, reviewing, and/or implementing Lean Six Sigma program;
b. Advising on, reviewing, and/or implementing Business Process reengineering;
c. Advising on, reviewing, and/or implementing DSC Process Optimization;
d. Advising on, reviewing, and/or producing DSC Process and operational training.

4.1.4. **Specific to a Supply Chain Business Activity**

1. Plan
   a. Advising on, reviewing, and/or implementing DSC Planning & Forecasting strategies and activities.

2. Acquisition
   a. Advising on, reviewing, and/or implementing Vendor-Managed Inventory within the DSC.

3. Distribution
   a. Advising on, reviewing, and/or producing DSC network design.

4. Warehousing
   a. Advising on, and/or reviewing DSC infrastructure asset investment alternatives and alternate means of operating the asset;
   b. Advising on, reviewing, and/or implementing short, medium, and long-term warehousing strategies;
   c. Advising on, reviewing, and/or implementing inventory segmentation.

5. Support
   a. Advising on, reviewing, and/or implementing Repair and Overhaul and reverse logistics processes.

6. Divestment
   a. Advising on, reviewing, and/or implementing divestiture, disposal, and ongoing asset and portfolio management activities related to major DSC infrastructure assets.

4.2. Deliverables (examples)

4.2.1. Various reports resulting from the tasks and activities listed under 4.1, such as but not limited to:

a. recommendation reports;
b. requirements documentation;
c. economic and risk analysis;
d. resource assessment reports (financial, personnel, equipment, infrastructure);
e. implementation plans;
f. capability roadmaps;
g. transformation roadmaps;
h. briefs;
i. plans;
j. gap analysis;
k. data compilations.

4.2.2. Presentations;

4.2.3. Agendas and minutes for meetings and conferences;

4.2.4. Visit reports for all travel that occurs.

5. Current DSC Digital Environment

5.1. Defence Resource Management Information System (DRMIS)

Execution of DSC Activities and management of materiel is conducted principally in National Defence's SAP-based Enterprise Resource Planner (ERP), the Defence Resource Management Information System (DRMIS). This system has undergone significant customization over the previous 15 years, which creates challenges to maintaining accuracy and consistency in materiel data.

Current version of SAP (ECC 6.0) used for Materiel Management, Financial Information, Plant Maintenance, Warehouse Management, and Inventory Management.

5.2. Additional Applications

There are numerous complementing and independent applications that execute the full spectrum of supply chain activities:

5.2.1. National Movement and Distribution System (NMDS). Deployable automated web-based system that interfaces directly with the DRMIS and the Central Medical Equipment Depot (CMED) database. It is used to facilitate the movement of materiel between DND facilities, deployed units and civilian facilities providing support to DND. NMDS is capable of the following functions:

a. Completion of documentation related to the shipping process, including customs and Dangerous Goods (DG).
b. Providing information related to the shipping process such as carrier rates, DGs information, Controlled Technology Access and Transfer (CTAT) information, etc.
c. Tracing of shipments through the Consignment Authorization Release Form (CARF) tracing module.
d. Tracking of shipments through the In-Transit Visibility (ITV) module.
e. Capable of providing statistical data to be used as a source of information, validation or for planning through Discoverer.
f. Can be used as a strategic planning tool for the movement of materiel.

5.2.2. Distribution Resource Planning (DRP). DRP is a commercial off the shelf inventory management application designed to calculate the time-phased inventory requirements of an organization. It is a unified service parts management solution that aims to maximize service at minimum cost, ensuring that the right part is in the right place, at the right time.

5.2.3. Human Resources Management System (HRMS). HRMS Civ was launched on 31 October 2007 as a result of the GC HRMS 8.9 project to manage all Human Resources (HR) processes for DND civilian employees. HRMS Civ evolved from a Commercial Off-the-Shelf (COTS) product originally developed by Peoplesoft Inc. There are actually two HRMS systems in use by DND. Although the two systems function independently, all data are combined on a common data base at the end of each business day:

a. HRMS Civ is the HR management system for the civilian employees of DND; and
b. HRMS Mil is the HR management system for members of the CAF.

5.2.4. Fleet Management System (FMS). FMS is the primary fleet management tool for DND. It is mandatory for all transport organisations to provide required data entry in the system to maintain accurate data on all vehicles and to use FMS to account for transport activities. FMS provides real time reporting capability. It is used to capture data of the day-to-day operations of any CAF Transport organization. The three main business purposes of FMS are:

a. daily operational management;
b. statistical and policy reporting; and
c. performance measurement.

6. Support Provided by Canada

6.1. Government Furnished Information (GFI) may be provided and will be detailed in each requirement.

6.2. As required, DND will arrange meetings and interviews with DND Subject Matters Experts and provide access to DND installations.

7. Acceptance Process and Criteria

7.1. The acceptance process and criteria may vary and will be defined in each requirement.

8. Travel

8.1. The Supplier may be required to travel to various locations across Canada.

8.2. The requirement for any travel will be identified in each resulting contract.

9. Location of Work

9.1. These services will be rendered at the Supplier’s facility. On an as requested basis, the Supplier may also be required to attend meetings at various DND locations in the National Capital Region (NCR).

10. Language

10.1. Services and deliverables are to be provided in English.

ANNEX B, SECURITY REQUIREMENTS CHECK LIST

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-210242
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: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM (Mat) - DGMSSC
3. a) Subcontract Number / Numéro du contrat de sous-traitance: N/A	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant: N/A

4. Brief Description of Work / Brève description du travail

Request for Supply Arrangement (RFSA) for the provision of advisory services in support of the Defence Supply Chain (DSC) Management Activities.

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 :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
UNCLASSIFIED

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-210242
Security Classification / Classification de sécurité
UNCLASSIFIED

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

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

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

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

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

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

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

Special comments:
Commentaires spéciaux :

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-210242
Security Classification / Classification de sécurité
UNCLASSIFIED

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-210242
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	Date
Dennis Lam	DBM 2 - Procurement & Contracting	LAM, DENNIS 538 Digitally signed by LAM, DENNIS 538 Date: 2021.01.04 09:58:24 -05'00'	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-219-5185		dennis.lam@forces.gc.ca	4 January 2021

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	Date
Sasa Medjovic	Senior security analyst	MEDJOVIC SASHA 234	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-996-0286		sasa.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	Date
Caroline Laflamme-Lafleur	Senior Procurement Officer	LAFLAMME-LAFLEUR, CAROLINE 043	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-297-6317		caroline.laflamme-lafleur@forces.gc.ca	4 January 2021

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	Date
Kelly Mureta Contract Security Officer Tel: 613-941-0441 kelly.mureta@tpsgc-pwgsc.gc.ca		Mureta, Kelly Digitally signed by Mureta, Kelly Date: 2021.01.25 15:40:39 -05'00'	

ATTACHMENT 1 TO ANNEX B, IT SECURITY REQUIREMENTS DOCUMENT

1. Introduction

1.1 The IT Security Requirements Document. This "IT Security Requirements Document for Supply Arrangement W6369-210242/A" is being provided in accordance with the instructions for completion of Part C, Section 11.d of the Treasury Board Secretariat (TBS) Form 350-103 which states:

> "Will the supplier be required to use its IT systems to electronically process and/or produce or store PROTECTED and/or CLASSIFIED information and/or data? If Yes, the client department and/or organization will be required to specify the IT security requirements for this procurement in a separate technical document."

Each IT Security Requirements Document applies only to the contract it is written for; accordingly this "IT Security Requirements Document for Supply Arrangement W6369-210242/A" is specific to Supply Arrangement W6369-210242/A.

1.2 DND's IT Security Requirements. This document outlines the Department of National Defence's (DND) Information Technology (IT) security requirements for the electronic storage / processing / creation of this contract's Proprietary Information up to and including the level of Protected B.

1.3 Proprietary Information. The term "Proprietary Information" is defined - for this document only - as any government assets and/or Sensitive (Designated or Classified) information which is stored / processed / created by private organizations to fulfil a contract with DND where contract security is administered by the PSPC Contract Security Program (PSPC/CSP).

1.4 Connectivity Criteria for IT Link. In the event that the Information System (IS) used to electronically store / process / create this Proprietary Information is also required to electronically connect to DND's infrastructure (i.e. the Security Requirements Check List (SRCL) Part C, Section 11.e is checked as "YES"), a separate IT Link "Connectivity Criteria" document will be completed by the Project Officer (PO) for the DND Project Management Office (PMO), and this link will require validation and authorization from PSPC/CSP.

1.5 Layers of Security Protection. Security is based upon layers of protection; in order for IT security requirements to effectively safeguard information they must be preceded and supported by other aspects of security and their associated policies. Contracting efforts should be preceded by the implementation of physical, personnel, procedural, information, and IT security safeguards.

1.6 Additional Information. The Contract Security Manual (CSM), available from Public Services and Procurement Canada (PSPC), prescribes the procedures to be applied by Canadian-based organizations for the safeguarding of government information and assets. Additional security information is available on the internet from PSPC/CSP, as well as the Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (CCCS), and the Royal Canadian Mounted Police (RCMP).

2. Mandatory Prerequisites

2.1 *PSPC Validation*

2.1.1 Contract Security Manual (CSM). All well as the security requirements in the CSM, the additional requirements stated in this document must be met. Whenever there are two requirements for the same issue, the most stringent requirement must be applied.

2.1.2 Contractor Sites. The contractor must inform PSPC/CSP and the DND PO of all physical sites where this contract's Protected B Proprietary Information will be stored / processed / created. This includes any applicable main and/or alternate contractor offices, construction sites, back-up storage locations, partners, all levels of sub-contractors offices, etc.

2.1.3 Site Requirements. Every site used to electronically store / process / create this contract's Proprietary Information must be granted a Facility Security Clearance (FSC) as well as either a Designated Organization Screening (DOS) or a Document Safeguarding Capability (DSC), as applicable. Every site must also be cleared by PSPC/CSP prior to being authorized to electronically store / process / create Proprietary Information.

2.2 *Physical Security*

2.2.1 Facility Authorization. Storage / processing / creation of this contract's Proprietary Information must only be performed in facilities which have been authorized by the PSPC/CSP. All data must be stored / processed / created in a secure manner that prevents unauthorized viewing, access, or manipulation.

2.2.2 Physical Security Zones. In accordance with the RCMP's "*G1-026 Guide to the Application of Physical Security Zones*", the IS - identified herein for this document only as the Supply Chain Optimization Information System - will be installed and operating in an Operations zone or in a temporary Operations zone.

2.2.3 Proprietary Information Outside of Canada. Storage / processing / creation of Proprietary Information outside of Canada is not authorized under this contract.

2.2.4 Mobile Computing/Teleworking. Mobile computing/teleworking (MC-TW) involving the IS or Proprietary Information is, under the following conditions, authorized under this contract.

2.2.4.1 The MC-TW site must first be validated, inspected (where required), and authorized by PSPC/CSP.

2.2.4.2 The Company Security Officer (CSO) or the Alternate Company Security Officer (ACSO) must approve in writing each Contractor employee's use of MC-TW.

2.2.4.3 Prior to starting MC-TW the Contractor employee must:

2.2.4.3.1 hold - at minimum - a valid Reliability Status which has been granted by PSPC/CSP;

2.2.4.3.2 have attended an IT security awareness training session/briefing, as required by the "IT Security Awareness Training" para of the "IT Security Requirements Document for Supply Arrangement W6369-210242/A"

2.2.4.3.3 have signed a User Agreement form, as required by the "User Agreement Form" para of the " Supply Arrangement W6369-210242/A IT Security Requirements Document"; and this User Agreement must include requirements and restrictions concerning MC-TW.

2.2.4.4 The use of Bluetooth Technology for or near the MC-TW IT equipment is prohibited.

2.2.4.5 The Contractor employee is not authorized to process, produce, send, receive, and/or store emails containing Supply Arrangement W6369-210242/A Proprietary information via smart phone;

2.2.4.6 When using MC-TW the Contactor and the Contractor employee must follow the tips in the following CSE publications:

2.2.4.6.1 "Security Tips for Organizations With Remote Workers (ITSAP.10.016)" (https://www.cyber.gc.ca/en/guidance/telework-security-issues-itsap10016); and

2.2.4.6.2 "Cyber Security Tips for Remote Work (ITSAP.10.116)" (https://cyber.gc.ca/en/guidance/cyber-security-tips-remote-work-itsap10116).

2.2.4.7 Details on the following must be documented for each MC-TW Contractor employee:

2.2.4.7.1 the type of IT equipment to be used. For example

2.2.4.7.1.1 thin client (a dumb terminal unit); or fat client (PC, laptop, tablet, etc.); and

2.2.4.7.1.2 the Contractor's company-owned computer or the Contractor employee's personally-owned computer;

2.2.4.7.2 the highest sensitivity level of data to be processed by the Contractor employee;

2.2.4.7.3 verification that the IT equipment used for MC-TW will be installed and operating in a temporary Operations Zone (minimum), in accordance with the RCMP's "*G1-026 Guide to the Application of Physical Security Zones*" (https://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-026-eng.htm);

2.2.4.7.4 the type of account to be used for the remote work (e.g. user, super user, administrator, etc.);

2.2.4.7.5 how the Proprietary Information is to be uploaded to/downloaded from the IT equipment (e.g. via VPN connection, or using removable media (USB sticks, CDs/DVDs, etc.);

2.2.4.7.6 the type of encryption to be used (if applicable) and the method of accessing the VPN;

2.2.4.7.7 encryption requirements for the hard drive and removable media, and/or password protection for the individual data files;

2.2.4.7.8 the physical location(s) where the MC-TW will take place (e.g. the Contractor employee will be working from his/her residence or from another

location); public spaces such as restaurants, coffee shops, stores etc. with public Wi-Fi are not allowed for teleworking; and

2.2.4.7.9 the number of computers/devices that each Contactor employee will be using for MC-TW. Tools for securing computing devices when not in use must be provided to the Contractor's employee.

2.2.4.8 The IT equipment must have a supported anti-virus/anti-malware application installed and operating with current anti-virus definition files which are to be updated at least every two days. The IT equipment must have all current Operating System security patches installed and kept up to date.

2.2.4.9 The applicable paras of the following sections of the "IT Security Requirements Document for Supply Arrangement W6369-210242/A" must be adhered to during MC-TW:

2.2.4.9.1 Information Security;

2.2.4.9.2 Authorization and Access Control; and

2.2.4.9.3 IT Media.

2.3 *Personnel Security*

2.3.1 Security Screening Level of Personnel. All contractor personnel who have access to any Proprietary Information must:

2.3.1.1 hold - at minimum - a valid Reliability Status which must be granted and be tracked by PSPC/CSP; and

2.3.1.2 be assigned system privileges on the criteria of least privilege; this means applying the most restrictive set of privileges and the need-to-know principle (i.e. limiting access to information only to those whose duties require such access) necessary for the performance of authorized tasks.

2.3.2 Access to the Physical Security Zone. No visitors, foreign nationals or unauthorized personnel shall have access to the Proprietary Information, the Supply Chain Optimization Information System, or the zone where the Proprietary Information is being stored / processed / created unless they possess a valid Reliability Status and are escorted by an authorized contractor employee. An audit log must be maintained of all visitors, foreign nationals or unauthorized personnel accessing the Operations zone.

2.3.3 IT Security Awareness Training. All contractor personnel handling Proprietary Information must be provided training and/or briefing sessions coordinated and delivered by the CSO or the ACSO. This training must, at minimum, make reference to the Government of Canada (GC) "Contract Security Manual" (CSM) and other security information as determined by the DND PO, as well as the system-specific IT Security Orders and Standard Operating Procedures (SOP) for the Supply Chain Optimization Information System. Training should also cover social engineering, use of social media, and situational awareness.

2.4 *Procedural Security*

2.4.1 IT Security Orders and Standard Operating Procedures. The contractor must create system-specific IT Security Orders for IS as well as SOPs relating to the operation and

maintenance of the Supply Chain Optimization Information System. These documents must be provided upon request, and must - at minimum - address:

2.4.1.1 roles and responsibilities (e.g. CSO, technical authority, IS system administrator(s), etc.);

2.4.1.2 access management for the Operations zone and the IS;

2.4.1.3 acceptable use of the IS;

2.4.1.4 incident management procedures;

2.4.1.5 any other subject identified in this document and

2.4.1.6 any other issue(s) identified by the DND PO or the DND PMO.

2.4.2 User Agreement Form. All personnel having access to the IS must read the system-specific IT Security Orders for the Supply Chain Optimization Information System and sign an associated User Agreement Form, as produced and tracked by the CSO or ACSO. All changes to the system-specific IT Security Orders, SOPs and/or User Agreement Form must be promulgated to all personnel having access to the IS.

2.4.3 System Administrator - Personnel Security Screening Level. The IS must be administered and maintained internally by individual(s) possessing - at minimum - a valid Reliability Status.

2.4.4 IS Continuous Monitoring. The contractor must continually monitor its overall security posture including physical, personnel, procedural, information, and IT security. The contractor must inform PSPC/CSP and the DND PO of any issues that could potentially impact the security of the Proprietary Information or the IS.

2.5 *Information Security*

2.5.1 Document Marking. All documents - hardcopy (paper) and softcopy (electronic) - containing Proprietary Information must be marked with the highest security level of the information contained in the document, and be afforded a unique identifier to ensure positive control and tracking.

2.5.2 Information at Rest. The contractor must protect the security of the Proprietary Information at rest through physical and/or IT security measures.

2.5.2.1 When unattended, all hardcopy (paper) documents containing Proprietary Information (e.g. paper printouts, etc.) must be physically locked in GC-approved security container(s) appropriate to the information's sensitivity level. The container(s) must be in accordance with the RCMP's "G1-001 - Security Equipment Guide"; as this Guide is not available to the general public, the contractor can contact the DND PO for information.

2.5.2.2 When unattended all removable IT media used to store / process / create Proprietary Information must be physically locked in GC-approved security container(s), as detailed in the RCMP's "G1-001 - Security Equipment Guide". Alternatively the removable media must be encrypted using GC-approved encryption technology appropriate for the sensitivity level of the Proprietary Information it contains.

2.5.2.3 Only contractor personnel authorized to have access to the Proprietary Information will be given the means to unencrypt electronic documents and/or have access to the key(s) and/or combination(s) for the approved secure container(s).

2.5.3 Exchange of Proprietary Information. When exchanging Proprietary Information between DND and all levels of contractors/sub-contractors via hard copy and/or removable IT media, all hard copy documents and removable IT media must be handled and transported/transmitted in accordance with GC guidelines as depicted in the CSM or the RCMP's "*G1-009 Transport and Transmittal of Protected and Classified Information*". When transported (i.e. hand carried from one person/place to another by an individual who has the need-to-know and is screened to the highest level of the Proprietary Information) or transmitted (i.e. sent from one person/place to another by a third party), all electronic media must be encrypted using GC encryption technology approved for the sensitivity level of the information contained in the electronic media.

2.5.4 Exchange of Proprietary Information - Packaging. All hard copy documents and IT media must be packaged appropriately and transported/transmitted with a covering letter as well as a transmittal form or circulation slip which must indicate:

2.5.4.1 the highest sensitivity level of information contained in the package;

2.5.4.2 the date of transport/transmission;

2.5.4.3 the unique identifier for each document/IT media in the package;

2.5.4.4 the printed name and phone number of the originator;

2.5.4.5 the signature of the originator

2.5.4.6 the physical street address of the destination;

2.5.4.7 the printed name and phone number of the recipient; and

2.5.4.8 the signature of the recipient.

2.5.5 Authorization of IT Link. Exchange of Proprietary Information with partners, sub-contractors or DND must not be done via IT links.

2.5.6 Segregation of Proprietary Information for Emergency Destruction. All Proprietary Information (e.g. hard copy documents, IT media, etc.) must be segregated from other contractual and corporate information in a way that allows all Proprietary Information to be securely destroyed or wiped, immediately upon request from PSPC/CSP or the DND PO as indicated in the CCCS publication "*IT Media Sanitization (ITSP.40.006)*".

2.5.7 Controlled Goods. For this contract, the contractor will not require access to Controlled Goods information or equipment.

2.5.8 Sub-contractors. The contractor must inform the DND PO and officially register with PSPC/CSP any partners and all levels of partnership and sub-contractors involved in this contract. The contractor is ultimately responsible for ensuring that all security requirements and all relevant and/or associated security documentation relating to this contract are provided to the contractor's partners and all levels of sub-contractors.

2.5.9 IT Security Requirements for Sub-Contracts. All applicable IT security requirements in this contract must also be included in any sub-contracts.

3. Minimum IT Security Requirements

3.1 *IT Security Policy Compliance and Monitoring*

On a frequency and schedule to be determined by the DND IT Security Authority, DND retains the right to conduct inspections of every contractor's facility involved in this contract to ensure compliance with the IT Security requirements herein as well as compliance with GC standards and policies concerning the prevention, detection, response, and recovery requirements.

3.2 *IT System Configuration*

3.2.1 Basic system configuration. The basic system configuration is anticipated by the DND PO to be one or more networked workstations (PCs or laptops) with access to local colour or black/white printers and the Internet. Information can be uploaded to/downloaded from the system using removable media (CDs/DVDs and USB sticks). An Air Gap Computer will be used to scan this removable media for viruses and malware.

3.2.2 Type of System. The IS can be configured as a segment of a network.

3.2.3 Segregation of IS. If configured as a segment of the contractor's corporate network, the contractor must segregate its corporate network into IT security zones and implement perimeter defence and network security safeguards. CSE and CCCS provide guidelines on this specific subject; see "*Network Security Zoning - Design Considerations for Placement of Services within Zones (ITSG-38)*" and "*Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)*". Details on segregation methodology (i.e. topology diagram and other documents as deemed necessary) must be provided to PSPC/CSP and the DND PO for evaluation. The contractor must also implement perimeter defence and network security safeguards for the IS to negotiate all traffic and to protect servers that are externally accessible.

3.2.4 Type of Equipment. The equipment used to store / process / create the Proprietary Information can consist of Commercial Off The Shelf (COTS) equipment and must be labelled commensurate with the highest sensitivity level of Proprietary Information to be processed on the equipment.

3.2.5 IS Hard Drives. Processing equipment can be configured with internal hard drives. Examples of processing equipment for this IS include workstations (PCs, laptops, tablets), servers, IT storage devices (network-attached storage (NAS), storage area network (SAN)), printers, scanners, etc.

3.2.6 Operating System. The IS must operate on a supported Operating System (OS); i.e. the vendor of the OS must be creating and providing current security patches for the OS. OS security patches must be installed regularly, at least monthly. The OS must be configured to disable unnecessary processes, services, and ports. The IS SOP must provide details on the OS configuration and identify the frequency and the method used to update the OS security patches.

3.2.7 Anti-virus/Anti-malware Software. A supported anti-virus/anti-malware application must be installed and operating on all workstations and servers (as applicable). Anti-virus/anti-malware definition files must be updated regularly and kept current. The IS SOP must provide details on the configuration of the anti-virus/anti-malware application as well as identify the frequency and the method used to update the anti-virus/anti-malware definition files. Configuration of the anti-virus/anti-malware application must:

3.2.7.1 allow changes to be made only by the system administrator(s);

3.2.7.2 automatically scan all Supply Chain Optimization Information System workstations/servers at power-on or on a set interval, at least weekly; and

3.2.7.3 scan every new file introduced to the IS workstations/servers for malicious code.

3.2.8 Software and Applications. Only applications required under this contract must be installed on the IS. Application patches must be kept up-to-date and be managed through a defined configuration management process. The IS SOP must list every installed application and its version, as well as identify the application patch management process.

3.2.9 Logging and Auditing. OS logging must be active and the log files must be reviewed by the Supply Chain Optimization Information System system administrator(s) at least monthly. The review must consist of - but not be limited to - successful logins; unsuccessful login attempts; unauthorized changes to the system hardware, firmware, and software; unusual system behaviour; unplanned disruption(s) of systems and/or services; system errors; etc. Only the system administrator(s) shall be allowed to modify or delete log files and only after being authorized by the CSO or ACSO. The IS SOP must identify the frequency and the method used to review the OS log files.

3.3 *IT Equipment*

3.3.1 Equipment Inventory. A list of all equipment forming the IS must be maintained by the contractor. This equipment list must contain - at minimum - the equipment's description, make, model, and quantity. If requested, this equipment list must be made available to PSPC/CSP and the DND PO.

3.3.2 Changes to IT Equipment. The contractor must inform PSPC/CSP and the DND PO of any major change(s) to the Supply Chain Optimization Information System IT equipment.

3.3.3 Wireless or Wi-Fi. The use of wireless or Wi-Fi capabilities on the IS is authorized under the following conditions:

3.3.3.1 the wireless of WI-FI capabilities must use, minimum, 128-bit encryption;

3.3.3.2 best practices as outlined in CSE's "ITSG-41, Security Requirements for Wireless Local Area Networks" must be followed;

3.3.3.3 modification of wireless/WI-FI settings is not authorized at the user level;

3.3.3.4 any modifications are to be done only by the system administrator(s) and only after advising the DND PO; and

3.3.3.5 the wireless/WI-FI to be used must first be validated, inspected and authorized by CISD.

3.3.4 Cloud Technology. The use of "cloud" technology to store / process / create Proprietary Information is strictly prohibited.

3.3.5 Network Interconnectivity. All network equipment interconnectivity:

3.3.5.1 must/can use minimum CAT 6 cabling or fibre optic cabling to connect the IS equipment;

3.3.5.2 must be identifiable from any other system wiring;

3.3.5.3 must be controlled and monitored to prevent inadvertent or deliberate connection to any unauthorized equipment, network or infrastructure; and

3.3.5.4 must/can be installed in the corporate wiring infrastructure.

3.3.6 Topology Diagram. A topology diagram of the Supply Chain Optimization Information System must be provided, upon request, to PSPC/CSP and/or the DND PO. The diagram must consist of a high-level system design and include any IT links to other entities and/or connections to other networks and/or systems, where applicable.

3.3.7 IT Equipment Maintenance and Disposal. Maintenance and disposal of any IT equipment used to store / process / create Proprietary Information (e.g. workstations, servers, printers, plotters, scanners, photocopiers and/or Multi-Function Devices (MFDs)/Multi-Function Printer (MFPs), etc.) must follow the instructions provided in the “Disposal” section, below.

3.4 *Authorization and Access Control*

3.4.1 List of Authorized Personnel. The contractor must maintain a list of authorized individuals who have access to the IS. This list must be updated whenever there is a change of personnel or a change to an individual's information that is contained on the list. The list must include, at minimum:

3.4.1.1 the individual's name

3.4.1.2 the individual's approved clearance level;

3.4.1.3 the date the individual's clearance expires; and

3.4.1.4 the type of access (e.g. user, power user, administrator, etc.).

3.4.2 System Accounts.

3.4.2.1 An individual Administrator account must be created for each system administrator. If an individual requires both administrator access and regular user access, the individual must have two separate accounts on the IS. Administrator accounts must not be used for standard day-to-day operations or non-administrative issues.

3.4.2.2 An individual User account must be created for each user; each account must have a unique name/identifier, and this name/identifier cannot be used by any other account holder for the life of the system. User accounts must be configured for limited privileges and must allow access only to the files and folders required by the user to perform their specific duties.

3.4.2.3 The IS must not contain:

3.4.2.3.1 any generic accounts,

3.4.2.3.2 any guest accounts,

3.4.2.3.3 any temporary accounts, or

3.4.2.3.4 shared accounts of any kind.

3.4.3 Passwords.

3.4.3.1 Each account must be protected by a password with an enforced minimum password complexity, as follows:

3.4.3.1.1 the password must contain a minimum of eight (8) characters;

3.4.3.1.2 the password must contain three of the following four criteria:

- at least one uppercase letter (A through Z),
- at least one lowercase letter (a through z),
- at least one number (0 through 9), and
- at least one special character (e.g. !, $, #, %);

3.4.3.1.3 password lifetime restrictions: minimum of one day and maximum of 90 days;

3.4.3.1.4 password reuse is prohibited for the previous ten (10) passwords; and

3.4.3.1.5 the account must lock after four (4) consecutive failed logon attempts.

3.4.3.2 Any password used to access the IS must:

3.4.3.2.1 be changed at first login;

3.4.3.2.2 be changed whenever there is any suspicion of compromise;

3.4.3.2.3 not be saved or remembered by the OS or any application accessed by the OS; and

3.4.3.2.4 never be shared with anyone.

3.4.3.3 The original local administrator password on all IT equipment forming the IS must be changed; vendor default passwords must not be used. Each time a local administrator password is changed it must be written down and placed in a sealed envelope which has been signed and dated over the flap by the CSO, ACSO or system administrator. The envelope must be locked in an approved container and safeguarded commensurate with the highest sensitivity level of data processed on the system.

3.4.4 IS Access Control List. All network elements (physical and/or virtual) of the IS must be tracked and be accessible (e.g. via access control list (ACL), Active Directory, etc.) only to authorized personnel.

3.4.5 Authorization and Access Control in SOP. The IS SOP must include an Authorization and Access Control process depicting the procedures for adding, disabling, and deleting user accounts.

3.5 *IT Media*

3.5.1 Disposal of IT Media. Throughout the duration of this contract, all IT media used to store / process / create Proprietary Information must be disposed of in accordance with the "Disposal" section of this document.

3.5.2 Removal of IT Media. In the event that equipment requires maintenance, support or replacement, **no IT media containing any Proprietary Information** (e.g. internal hard drives, removable IT media, etc.) will be given or made available to any outside vendor, service provider or other unauthorized personnel.

3.5.3 Identification of IT Media. All IT media (e.g. internal hard drives, removable hard drives, external hard drives, CDs/DVDs, USB sticks, etc.) used to store / process / create Proprietary Information must:

3.5.3.1 be dedicated to this contract only;

3.5.3.2 be given a unique identifier to ensure positive control and tracking;

3.5.3.3 be identified and inventoried by:

3.5.3.3.1 the type of media (e.g. CD/DVD, USB stick, etc.);

3.5.3.3.2 the information sensitivity level,

3.5.3.3.3 the release-ability caveat (if applicable),

3.5.3.3.4 the model and serial number (if applicable), and

3.5.3.3.5 the IT media's unique identifier;

3.5.3.4 be labelled with:

3.5.3.4.1 the highest sensitivity level of the data it contains,

3.5.3.4.2 the government department (in this case DND),

3.5.3.4.3 the contract number, and

3.5.3.4.4 the IT media's unique identifier.

3.5.3.5 If a label cannot be affixed directly on the IT media, the label must be attached to the IT media by other means (e.g. string, etc.).

3.5.4 Safeguarding of IT Media. All IT media must be safeguarded commensurate with the highest sensitivity level of the data it contains. When not being used all removable IT media - including failed, life cycled and long-term use media (e.g. backup media, etc.) - must be locked in a secure container approved to the information sensitivity level of the data that it contains.

3.5.5 Air Gap Computer. If the IS is required to interact with untrusted sources (e.g. the internet, another network, removable IT media from another source, etc.) the contractor will be required to provide a standalone Air Gap computer. Data transfer security requirements and related instructions for the Air Gap computer will be provided by the DND PO in a separate technical document; a template for this is available from DIM Secur upon request.

3.5.6 Logging of Removable IT Media. The location of all removable IT media must be tracked and controlled via the use of a log book. The log book must contain, at minimum:

3.5.6.1 the type of media (e.g. CD/DVD, USB stick, removable hard drive, backup tape, etc.);

3.5.6.2 the IT media's unique identifier;

3.5.6.3 the date and time it was removed;

3.5.6.4 the name, or initials, and signature of the individual who signed it out;

3.5.6.5 the date and time it was returned; and

3.5.6.6 the name, or initials, and signature of the individual who returned the media.

3.6 ***Document Printing and/or Reproduction***

3.6.1 Printing/Reproduction Authorization. The contractor is:

3.6.1.1 authorized to print and/or reproduce any Proprietary Information within the contractor’s premises; and

3.6.1.2 not authorized to use external printing and/or reproduction services. External printing and/or reproduction must be addressed through sub-contract(s).

Use of either of these services to print and/or reproduce any Proprietary Information must first be approved and authorized by PSPC/CSP and the DND PO.

3.6.2 Printing/Reproduction Device Hard Drives. Devices used to reproduce Proprietary Information (e.g. printers, plotters, scanners, photocopiers, MFDs/MFPs, etc.) can be equipped with internal hard drives.

3.6.3 Printer Connections. Unless the IS is configured as a segment of the contractor's corporate network, all printers, plotters, scanners, photocopiers and/or MFDs/MFPs must only be connected to the IS. Connection to other devices or networks is strictly prohibited.

3.6.4 Connection of Telephone Lines. The connection of telephone lines to any MFD/MFP used to process Proprietary Information is strictly prohibited.

3.6.5 Reproduction of Particularly Sensitive Information. For any particularly sensitive Proprietary Information, printing/reproduction of each document must first be approved by the DND PO; and if approved, every copy must be afforded a unique identifier to ensure positive control and tracking.

3.7 *Recovery*

3.7.1 IS Backups. The Proprietary Information must be backed up regularly, at least once a week; and the backups must be safeguarded at a remote location (i.e. another building). If the contractor does not have a remote location to safeguard the backups, arrangements can be made with the DND PO. If backups are to be safeguarded by a private organization other than the contractor, this must be addressed though a sub-contract. The IS SOP must include details on the back-up frequency, methodology and storage.

3.7.2 Testing of Backups. The IS backups should be tested on a regular basis. The IS Standard Operating Procedures should include details on the back-up testing frequency, methodology and reporting of errors.

3.7.3 Disaster Recovery Plan. The contractor must develop, and document a Disaster Recovery Plan (DRP) for the IS. This DRP must include details on the recovery, restoration, testing frequency, and methodology.

3.8 *Disposal*

3.8.1 Authorization for Disposal. The disposal of all IT media used on this contract - including removable media, internal and external hard drives - must be authorized in advance by the DND PO and must be documented and tracked. This includes for example, IT media that has failed, is being life cycled, is no longer required, etc. If hard drives cannot be removed from devices used to store / process / create Proprietary Information (e.g. tablets, etc.) then the devices must be returned to the DND PO.

3.8.2 On-Site Disposal. If the contractor does not have the required disposal means, arrangements can be made with the DND PO for disposal of IT media. If disposal of IT media is prohibited at the contractor's site the contractor must make arrangements for disposal with the DND PO. Disposal of IT media on-site at the contractor's facility is authorized under the following condition:

3.8.2.1 the contractor must dispose of IT media in accordance with CSE's "ITSP.40.006 - IT Media Sanitization".

3.8.3 Disposal of IT Media - Tracking. The disposal of IT media must be tracked via the use of a "Certificate of Destruction" (if applicable) and a "Transit and Receipt Form"; the DND PO will provide templates for these documents. The contractor must retain a copy of all IT disposal documents as evidence that the IT media has been properly disposed of. The contractor must make these IT disposal documents available to PSPC/CSP and the DND PO upon request.

3.8.4 Return of All Proprietary Information. At the end of the contract all Proprietary Information (hard copies and electronic) must be returned to the DND PO. This includes all paper copies of documents as well as any IT media used to store / process / create Proprietary Information (e.g. internal hard drives (used in workstations, laptops, servers, photocopiers, MFDs/MFPs, etc.); CDs/DVDs; USB sticks; SD cards; external hard drives; etc.). If hard drives cannot be removed from devices used to store / process / create Proprietary Information (e.g. tablets, etc.) then the devices must be returned to the DND PO.

3.8.5 Procedures Prior to Removal of IT Equipment. If maintenance and/or disposal of IT equipment is necessary, the following procedures must be applied prior to removing any IT equipment used to store / process / create Proprietary Information; this process applies to all IT equipment containing IT media (e.g. servers, workstations, printers, plotters, scanners, MFDs/MFPs, etc.):

3.8.5.1 All non-volatile memory devices (internal, removable, and external hard drives, etc.) must be removed and be disposed of as indicated in this section.

3.8.5.2 Volatile memory (e.g. RAM, DRAM, SRAM, etc.) must be sanitized by removing all power for a minimum of 24 consecutive hours. The contractor must ensure there is no power to the memory (e.g. from internal batteries or through connection to another device). If there is any doubt concerning the removal of all power to volatile memory in equipment used to store / process / create highly sensitive Proprietary Information, the contractor must remove the volatile memory from the device and have it destroyed.

3.8.5.3 Any stickers or security markings on the device - in connection with this contract or the IS - must be removed.

ATTACHMENT 2 TO ANNEX B, AIR GAP COMPUTER DOCUMENT

1. Introduction

1.1 This document outlines the Information Technology (IT) security requirements for Department of National Defence (DND) Supply Arrangement W6369-210242/A for the transfer of electronic information between the Information System (IS) - identified herein for this document only as the Supply Chain Optimization Information System - used to process, produce, and/or store this contract's Proprietary Information up to and including the level of Protected B. The scope of this "Air Gap Computer Document for Supply Arrangement W6369-210242/A" is to state the minimum IT security requirements necessary to transfer electronic information to and from the IS.

1.2 Throughout this document the term “Proprietary Information” is defined - as paraphrased from Section 1.1 of the PSPC’s Contract Security Manual (CSM), - as: "any government information and/or assets, provided to or produced by private organizations and where security is administered by the PSPC Contract Security Program."

1.3 As this contract may require data inputs from untrusted sources, there is a need for an additional level of IT security to mitigate the possibility of infection or malware originating from untrusted sources. These extra steps are intended to protect not only the Supply Chain Optimization Information System but also any other system exchanging information with the IS. The transfer of all Proprietary Information into the IS will be required to transition through an Air Gap Computer.

1.4 The application of the IT security safeguards listed in this document are based on the mandatory requirement that the physical premises have been inspected, assessed and authorized to process, produce and/or store information up to and including Protected B. Validation must be provided by the Public Services & Procurement Canada (PSPC)/ Contract Security Program (CSP).

2. Mandatory Prerequisites

2.1 *Description*

2.1.1 A standalone workstation (i.e. PC or laptop) equipped with a removable hard drive as well as two approved and supported anti-virus/anti-malware applications must be used for all electronic data transfers into the IS. The transfer of electronic data into this IS is allowed only from a system of equivalent sensitivity level or lower.

2.1.2 The transfer of electronic data from the Supply Chain Optimization Information System must first be authorized in writing by the DND Project Officer (PO).

2.2 *Terminology*

2.2.1 The following terminology will be used in this document.

Source File	The data to be transferred to the Target System; the Source File must not have a higher sensitivity level than the Target System.
Source System	The IS that the Source File came from.

Target System	The IS that the Source File will be uploaded to. The Target System is the Supply Chain Optimization Information System.
Source Transfer Media	The removable electronic media (e.g. CDs/DVDs, USB sticks, SD cards, external hard drives, etc.) containing the Source File from the Source System. For the Supply Chain Optimization Information System the type(s) of Source Transfer Media will be CDs/DVDs and USB sticks, as well as any other type(s) of removable media approved in writing by the DND Project Authority.
Target Transfer Media	The removable electronic media to be used to move the Source File from the Supply Arrangement W6369-210242/A Air Gap Computer to the Target System. For the Supply Chain Optimization Information System the type(s) of Target Transfer Media will be CDs/DVDs and USB sticks, as well as any other type(s) of removable media approved in writing by the DND Project Authority.

2.3 ***Hardware***

2.3.1 This Air Gap Computer must consist of a stand-alone PC or laptop with only a monitor, keyboard and mouse. No other peripheral equipment (e.g. printer, scanner, etc.) can be attached to the Air Gap Computer.

2.3.2 For the entire length of the contract, this Air Gap Computer must be used only for this purpose.

2.3.3 This Air Gap Computer must be owned by the contractor; be composed of Commercial-Off-the-Shelf (COTS) equipment; and be installed, configured, and operational before being inspected by PSPC/CSP.

2.3.4 If using a PC, the Air Gap Computer must be equipped with a removable hard drive.

2.3.5 This Air Gap Computer must be installed and operating in the same Operations zone or the temporary Operations zone where the Supply Chain Optimization Information System is installed.

2.3.6 If processing Protected C and/or Classified data, this Air Gap Computer must be located at least one meter away from all IT equipment and all personal IT devices (PITDs).

2.3.7 Labelling. This Air Gap Computer and removable hard drive (if applicable) must be affixed with a label identifying the highest sensitivity level of the contract's Proprietary Information which is being transferred using this equipment.

2.3.8 Labelling of Transfer Media. The Transfer Media to be used on this Air Gap Computer must be marked with the following information:

2.3.8.1 the highest sensitivity level of the data it contains,

2.3.8.2 the government department (in this case DND),

2.3.8.3 the contract number,

2.3.8.4 the IT media's unique identifier, as discussed in para 3.5.3.2 of the "Supply Arrangement W6369-210242/A IT Security Requirements Document", and

2.3.8.5 the transfer media category (either "Source Transfer Media" or "Target Transfer Media").

2.3.9 If this information cannot be written directly on the media or if a large label (approximately 4" by 6") cannot be affixed directly on the media, the label must be attached to the IT media by other means (e.g. string, etc.).

2.3.10 The "Source Transfer Media" and the "Target Transfer Media" should be labelled with different colours (e.g. black for one, red for the other) to easily differentiate between them.

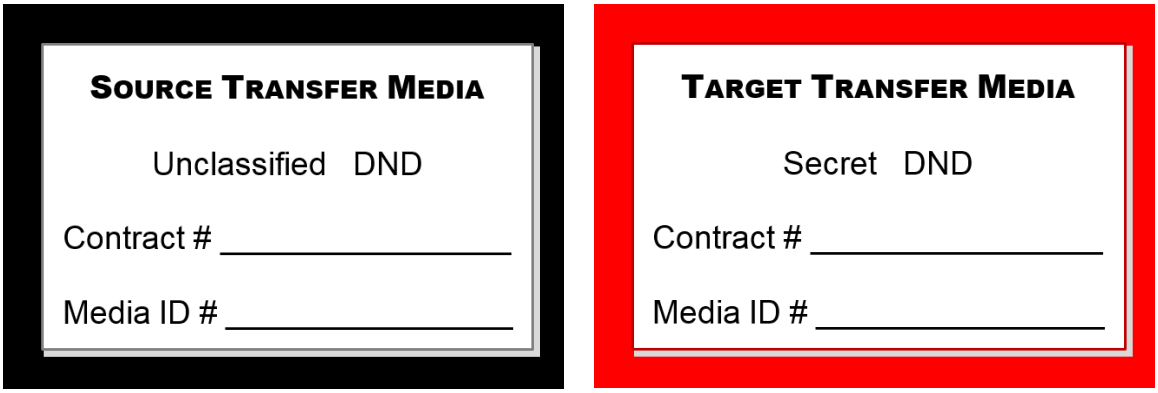

Figure 1: example labels

2.4 *IT System Configuration*

2.4.1 This Air Gap Computer must operate on a supported Operating System (OS) and must follow all items specified in the paragraph "Operating System" of the "Supply Arrangement W6369-210242/A IT Security Requirements Document". As well as disabling unnecessary processes, services, and ports, all unnecessary computer components (e.g. network card, microphone, speakers, etc.) must also be disabled.

2.4.2 Two different anti-virus/anti-malware applications must be installed on this contract's Air Gap Computer and these applications must be supported. This contract's Air Gap Computer must follow all items specified in the paragraph "Anti-virus/Anti-malware Software" of the "Supply Arrangement W6369-210242/A IT Security Requirements Document".

2.4.3 Any other applications installed on this contract's Air Gap Computer shall be deleted/uninstalled, and no other applications can be installed on this computer.

2.4.4 OS logging must be active on this contact's Air Gap Computer, and all items specified in the paragraph "Logging and Auditing" of the "Supply Arrangement W6369-210242/A IT Security Requirements Document" must be followed.

2.4.5 All accounts on this contact's Air Gap Computer must follow the applicable sections of the paragraph "Authorization and Access Control" of the "Supply Arrangement W6369-210242/A IT Security Requirements Document". No shared or generic accounts are authorized.

2.4.6 The following paragraphs of the "Supply Arrangement W6369-210242/A IT Security Requirements Document" are applicable to this Air Gap Computer and must be followed:

- "Unattended Removable Media";
- "IT Media";
- "Personal IT Devices (PITDs)"; and
- "Disposal".

2.5 *Air Gap Computer and SOP*

2.5.1 The Supply Chain Optimization Information System SOP must include the procedures and details mentioned in this "Air Gap Computer Document for Supply Arrangement W6369-210242/A" for all applicable aspects of this Air Gap Computer.

3. Data Transfer Procedures

3.1 The following process must be used to transfer electronic data from any untrusted source(s) to the IS.

3.2 These Data Transfer Procedures must be posted near the Supply Arrangement W6369-210242/A Air Gap Computer.

DATA TRANSFER PROCEDURES

1. Power on the Supply Arrangement W6369-210242/A Air Gap Computer and logon.
2. Ensure that the definition files for both anti-virus/anti-malware applications are current. If not current, update the necessary definition files before proceeding.
3. Copy the Source File(s) from the Source System to the Source Transfer Media. If the Source File(s) is/are already on removable electronic media (e.g. removable media received from a vendor, etc.), then this can be used as the Source Transfer Media.
4. Label the Source Transfer Media and connect it to the Air Gap Computer.
5. Scan the Source Transfer Media and all Source File(s) using both anti-virus/anti-malware applications.
    a. If any viruses/malware are detected, STOP the procedure. Clean/delete the file(s) as directed by the anti-virus/anti-malware applications and inform the Company Security Officer (CSO) or the Alternate Company Security Officer (ACSO).
    b. If no viruses/malware are detected, proceed to the next step.
6. Copy the Source File(s) from the Source Transfer Media onto the Air Gap Computer.
7. Remove the Source Transfer Media from the Air Gap Computer.
8. Label the Target Transfer Media and connect it to the Air Gap Computer.
9. Copy the scanned Source File(s) from the Air Gap Computer to the Target Transfer Media.
10. Remove the Target Transfer Media from the Air Gap Computer.
11. Connect the Target Transfer Media to the Target System.
12. Copy the scanned Source File(s) from the Target Transfer Media to the Target System.
13. Ensure that the scanned Source File(s) copied to the Target System can be opened and are not corrupted.
14. If the Source File(s) on the Target System is/are satisfactory:
    a. delete the Source File(s) from the Target Transfer Media;
    b. remove the Target Transfer Media from the Target System; and
    c. delete the Source File(s) from the Air Gap Computer.
15. Log off and shut down the Air Gap Computer.