National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

FINAL

# REQUEST FOR PROPOSAL / DEMANDE DE PROPOSITION

**RETURN BIDS TO / RETOURNER LES SOUMISSIONS À:**

Director Services Contracting (D Svcs C 3)
Attn: Lana Ibrahim, D Svcs C 3-4-2
By e-mail to: Lana.Ibrahim@forces.gc.ca

**Proposal To: National Defence Canada**

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods and services listed herein and on any attached sheets at the price(s) set out therefore.

**Proposition à: Défense nationale Canada**

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens et services énumérés ici et sur toute feuille ci-annexée, au(x) prix indique(s).

**Comments – Commentaires**

**THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT**
**CE DOCUMENT CONTIENT UNE EXIGENCE DE SÉCURITÉ.**

**Solicitation Closes / L'invitation prend fin:**

At / à:

2:00 PM Eastern Standard Time (EST)

On / le:

26 January 2023

| **Title / Titre** | **Solicitation No. / Nº de l'invitation** |
|---|---|
| Environmental Monitoring Systems (EMS) | W6369-22-A009 |

**Date of Solicitation / Date de l'invitation**
14 December 2022

**Address Enquiries to / Adresser toutes questions à:**

Lana Ibrahim, D Svcs C 3-4-2
Lana.Ibrahim@forces.gc.ca

| **Telephone No. / Nº de téléphone** | **FAX No. / Nº de fax** |
|---|---|

**Destination**

National Defence Headquarters
Central Medical Equipment Depot (CMED)
105 Montgomery Road, Building BB-104
Petawawa, Ontario
K8H 2X3

**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 harmonisée doit être indiqué séparément.**

| **Delivery Required / Livraison exigée** | **Delivery Offered / Livraison proposée** |
|---|---|

**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 _____

**TABLE OF CONTENTS**

Canada

## PART 1 - GENERAL INFORMATION

### 1.1 Introduction

A. The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

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

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

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

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

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

B. The Attachments include the Pricing Schedule, the Technical Evaluation, and any other attachments.

C. The Annexes include the Statement of Requirement, the Basis of Payment, the Security Requirements Checklist, and any other annexes.

### 1.2 Summary

A. The Department of National Defence (DND) has a requirement for the supply of Environmental Monitoring Systems (EMS) fitted with data loggers and alarms to continuously and remotely monitor the temperature of 2ºC to 8ºC refrigerators as well as -20ºC and -80ºC freezers deployed for the storage of COVID-19 vaccines. The goods must be delivered to Central Medical Equipment Depot (CMED) at 105 Montgomery Road, Ottawa Ontario.

The Initial Contract period will be from date of contract award to 31 March 2024. All deliverables must be received on or before 30 August 2023 for the Initial Contract period. Optional Requirement goods and services, required on an “as and requested” basis, must be delivered before 31 March 2027.

B. There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, Bidders 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.

C. The requirement is subject to the provisions of Canada-Chile Free Trade Agreement, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Canada-Colombia Free Trade Agreement, Canada European Union Comprehensive Economic and Trade Agreement (CETA), Canada-Honduras Free Trade Agreement, the Canada-Korea Free Trade Agreement, Canada-Panama Free Trade Agreement, Canada-Peru Free Trade Agreement, Canada-Ukraine Free Trade Agreement, Canada-United Kingdom Trade Continuity Agreement, the World Trade Organization Agreement on Government Procurement (WTO-AGP), and the Canadian Free Trade Agreement (CFTA).

**1.3 Debriefings**

A. Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

## PART 2 - BIDDER INSTRUCTIONS

### 2.1 Standard Instructions, Clauses and Conditions

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

B. Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

C. The 2003 (2022-03-29), Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation, with the following modification(s):

(i) Section 02, Procurement Business Number, is deleted in its entirety;

(ii) Section 05, Submission of bids, subsection 2, paragraph d., is deleted in its entirety and replaced with the following:

d. send its bid only to the Department of National Defence location specified on page 1 of the bid solicitation or to the address specified in the bid solicitation.

(iii) Section 05, Submission of bids, subsection 2, paragraph e., is deleted in its entirety and replaced with the following:

e. ensure that the Bidder's name, return address, the bid solicitation number, and bid solicitation closing date and time are clearly visible on the bid; and

(iv) Section 05, Submission of bids, subsection 3, is deleted in its entirety;

(v) Section 05, Submission of bids, subsection 4, is amended as follows:

Delete: 60 days
Insert: 180 days

(vi) Section 06, Late bids, is deleted in its entirety;

(vii) Section 07, Delayed bids, is deleted in its entirety and replaced with the following:

07 Delayed bids

1. It is the Bidder’s responsibility to ensure that the Contracting Authority has received the entire submission. Misrouting or other electronic delivery issues resulting in late submission of bids will not be accepted.

(viii) Section 08, Transmission by facsimile, is deleted in its entirety; and

(ix) Section 20, Further information, is deleted in its entirety.

### 2.2 Submission of Bids

A. Bids must be submitted only to the Department of National Defence (DND) by the date, time, and place indicated on page 1 of the bid solicitation.

B. Due to the nature of the bid solicitation, bids transmitted by facsimile will not be accepted.

### 2.2.1 Electronic Submissions

A. 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 Bidder or Contracting Authority. Larger bids may be submitted through more than one e-mail. Canada will confirm receipt of documents. It is the Bidder's responsibility to ensure that their entire submission has been received. Bidders 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, bidders are requested to allow sufficient time before the closing date and time to confirm receipt. Bid documents submitted after the closing time and date will not be accepted.

### 2.3 Enquiries - Bid Solicitation

A. All enquiries must be submitted in writing to the Contracting Authority no later than 10 calendar days before the bid closing date. Enquiries received after that time may not be answered.

B. Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders 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 the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

### 2.4 Applicable Laws

A. Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

B. Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, 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 Bidders.

### 2.5 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 - BID PREPARATION INSTRUCTIONS

### 3.1 Bid Preparation Instructions

A. Canada requests that Bidders provide their bid in separately bound sections as follows:

Section I: Technical Bid: one (1) soft copy in PDF format by e-mail;

Section II: Financial Bid: one (1) soft copy in PDF format by e-mail;

Section III: Certifications: one (1) soft copy in PDF format by e-mail; and

Section IV: Additional Information: one (1) soft copy in PDF format by e-mail.

B. Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

C. Canada requests that Bidders follow the format instructions described below in the preparation of their bid:

(i) Use 8.5 x 11 inch (216 mm x 279 mm) paper; and

(ii) Use a numbering system that corresponds to the bid solicitation.

### 3.2 Section I: Technical Bid

A. In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

B. The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

### 3.3 Section II: Financial Bid

A. Bidders must submit their financial bid in accordance with the Pricing Schedule detailed in Attachment 1 to Part 3.

#### 3.3.1 Electronic Payment of Invoices - Bid

A. If you are willing to accept payment of invoices by Electronic Payment Instruments, complete Attachment 2 to Part 3, Electronic Payment Instruments, to identify which ones are accepted.

B. If Attachment 2 to Part 3, Electronic Payment Instruments is not completed, it will be considered as if Electronic Payment Instruments are not being accepted for payment of invoices.

C. Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.

**3.3.2 Exchange Rate Fluctuation**

A. The requirement does not offer exchange rate fluctuation risk mitigation. Requests for exchange rate fluctuation risk mitigation will not be considered. All bids including such provision will render the bid non-responsive.

**3.4 Section III: Certifications**

A. Bidders must submit the certifications and additional information required under Part 5.

**3.5 Section IV: Additional Information**

A. In Section IV of their bid, bidders should provide:

(i) A completed, signed, and dated Page 1 of this solicitation;

(ii) The name of the contact person (provide also this person's title, mailing address, phone number, and email address) authorized by the Bidder to enter into communications with Canada with regards to their bid, and any contract that may result from their bid;

(iii) For Part 2, article 2.5, Applicable Laws, of the bid solicitation: the province or territory if different than specified;

(iv) For Part 6, article 6.1, Security Requirement, of the bid solicitation, for each individual who will require access to classified or protected information, assets, or sensitive work sites:

(a) the name of the individual;

(b) the date of birth of the individual; and

(c) if available, information confirming the individual meets the security requirement as indicated in Part 7 - Resulting Contract Clauses; and

(v) Any other information submitted in the bid not already detailed.

**3.5.1 Bidder's Proposed Sites or Premises Requiring Safeguarding Measures**

A. As indicated in Part 6 under Security Requirements, the Bidder must provide the full addresses of the Bidder's and proposed individuals' sites or premises for which safeguarding measures are required for Work Performance:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

B. The Company Security Officer (CSO) must ensure through the Contract Security Program that the Bidder and proposed individuals hold a valid security clearance at the required level, as indicated in Part 6 - Security, Financial and Other Requirements.

## ATTACHMENT 1 TO PART 3 - PRICING SCHEDULE

A. The Bidder must complete this pricing schedule and include it in its financial bid.

B. The volumetric data included in this pricing schedule are provided for bid evaluated price determination purposes only. They are not to be considered as a contractual guarantee. Their inclusion in this pricing schedule does not represent a commitment by Canada that Canada's future usage of the services described in the bid solicitation will be consistent with this data.

C. The firm rates specified below includes all expenses that may need to be incurred to satisfy the terms of any contract that may result from its bid, including the total estimated cost of any travel and living expenses that may need to be incurred for the Work described in Annex A, Statement of Work of the bid solicitation.

D. Under any resulting contract, Canada will not accept travel and living expenses that may need to be incurred by the contractor for any relocation of resources required to satisfy its contractual obligations.

E. All prices and costs must be submitted in Canadian Dollars, Applicable Taxes excluded, Delivered at Place (DAP), freight charges included, Canadian customs duties and excise taxes excluded.

### 1. Pricing Schedule

| **Currency** | CAD $ |
|---|---|

### 1.1 INITIAL CONTRACT PERIOD: FROM DATE OF CONTRACT AWARD TO 31 MARCH 2024. ALL ITEMS MUST BE DELIVERED BY 30 AUGUST 2023.

| ITEM NO. | DESCRIPTION | QTY | UNIT OF ISSUE | FIRM UNIT PRICE (CAD $) | TOTAL ESTIMATED PRICE (CAD $) |
|---|---|---|---|---|---|
| | | (A) | | (B) | (C = A x B) |
| **1.0** | **EQUIPMENT** | | | | |
| 1.1 | -80 ºC freezer probe-transmitter and its Certificate of Calibration testing, as referenced in Annex A, para 2.1.1.1 herein | Up to 5 | Each | $ | $ |
| 1.2 | -20ºC freezer probe-transmitter and its Certificate of Calibration testing, as referenced in Annex A, para 2.1.1.1 herein | Up to 30 | Each | $ | $ |
| 1.3 | 2 ºC to 8 ºC refrigerator probe-transmitter and its Certificate of Calibration testing, as referenced in Annex A, para 2.1.1.1 herein | Up to 61 | Each | $ | $ |
| 1.4 | Receivers-gateways fitted with Global | 1 | Lot | $ | $ |

| | | | | | |
|---|---|---|---|---|---|
| | System for Mobile communications (GSM) router, as referenced in Annex A, para 2.1.1.2 herein | | | | |
| 1.5 | Software package for all the probes-transmitters with unlimited number of users and unlimited alarms (phone, email, text), as referenced in Annex A, para 2.1.2.1 herein | 1 | Each | $ | $ |
| 1.6 | Cellular network plan for all the receivers-gateways as referenced in Annex A, para 2.1.2.2 herein | 1 | Each | $ | $ |
| **2.0** | **TRAINING** | | | | |
| 2.1 | Virtual Operator Training Session for 5 to 10 operators as described in Annex A, para 9.1 herein. | Up to 30 | Session | $ | $ |
| 2.2 | Technical Service Training for 2 to 8 Biomedical Engineering Technologists as described in Annex A, para 9.2 herein. | 1 | Session | $ | $ |
| | | | **TOTAL INITIAL CONTRACT PERIOD** | | **$** |

**2.0 OPTIONAL REQUIREMENTS FROM 01 APRIL 2024 TO 31 MARCH 2027. ALL ITEMS MUST BE DELIVERED BY 31 MARCH 2027.**

**2.1 OPTIONAL REQUIREMENT – YEAR 1: 01 APRIL 2024 TO 31 MARCH 2025**

| ITEM NO. | DESCRIPTION | QTY | UNIT OF ISSUE | FIRM UNIT PRICE (CAD $) | TOTAL ESTIMATED PRICE (CAD $) |
|---|---|---|---|---|---|
| | | (A) | | (B) | (C = A x B) |
| **1.0** | **EQUIPMENT** | | | | |
| 1.1 | Any type of probe-transmitter among -80 °C, -20°C, 2 °C to 8 °C, with its Certificate of Calibration testing, as referenced in Annex A, para 2.2.1.1 herein | Up to 24 | Each | $ | $ |
| 1.2 | Receiver-gateway fitted with Global System for Mobile communications (GSM) router, as referenced in Annex A, para 2.2.1.2 herein | Up to 6 | Each | $ | $ |

| | | | | | |
|---|---|---|---|---|---|
| 1.3 | Software package for one (1) additional probe-transmitter for one (1) year, as referenced in Annex A, para 2.2.3.1 herein | Up to 24 | Each | $ | $ |
| 1.4 | Cellular plan for one (1) additional receiver-gateway for one (1) year, as referenced in Annex A, para 2.2.3.3 herein | Up to 6 | Each | $ | $ |
| 1.5 | Software package for initial probes-transmitters as referenced in Annex A, para 2.2.3.2 herein | 1 | Each | $ | $ |
| 1.6 | Cellular network plan for initial receivers-gateways as referenced in Annex A, para 2.2.3.4 herein | 1 | Each | $ | $ |
| 1.7 | Offsite calibration of probes, as referenced Annex A, para 2.2.2.3 herein | 1 | Service | $ | $ |
| **2.0** | **TRAINING** | | | | |
| 2.1 | Virtual Operator Training Session for 5 to 10 operators per session as described in Annex A, para 9.1 herein. | Up to 10 | Session | $ | $ |
| 2.2 | Technical Service Training for 2 to 8 Biomedical Engineering Technologists per session as described in Annex A, para 9.2 herein. | 1 | Session | $ | $ |
| | | | | **TOTAL OPTION REQUIREMENT – YEAR 1:** | **$** |

**2.2 OPTIONAL REQUIREMENT – YEAR 2: 01 APRIL 2025 TO 31 MARCH 2026**

| ITEM NO. | DESCRIPTION | QTY | UNIT OF ISSUE | UNIT RATE (CAD$) | EXTENDED RATE (CAD$) |
|---|---|---|---|---|---|
| | | **(A)** | | **(B)** | **(C = A x B)** |
| **1.0** | **EQUIPMENT** | | | | |
| 1.1 | Any type of probe-transmitter among -80 °C, -20°C, 2 °C to 8 °C, with its Certificate of Calibration testing, as referenced in Annex A, para 2.2.1.1 herein | Up to 24 | Each | $ | $ |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| 1.2 | Receiver-gateway fitted with Global System for Mobile communications (GSM) router, as referenced in Annex A, para 2.2.1.2 herein | Up to 6 | Each | $ | $ |
| 1.3 | Software package for one (1) additional probe-transmitter for one (1) year, as referenced in Annex A, para 2.2.3.1 herein | Up to 48 | Each | $ | $ |
| 1.4 | Cellular plan for one (1) additional receiver-gateway for one (1) year, as referenced in Annex A, para 2.2.3.3 herein | Up to 12 | Each | $ | $ |
| 1.5 | Software package for initial probes-transmitters as referenced in Annex A, para 2.2.3.2 herein | 1 | Each | $ | $ |
| 1.6 | Cellular network plan for initial receivers-gateways as referenced in Annex A, para 2.2.3.4 herein | 1 | Each | $ | $ |
| 1.7 | Offsite calibration of probes, as referenced Annex A, para 2.2.2.3 herein | 1 | Service | $ | $ |
| **2.0** | **TRAINING** | | | | |
| 2.1 | Virtual Operator Training Session for 5 to 10 operators per session as described in Annex A, para 9.1 herein. | Up to 10 | Session | $ | $ |
| 2.2 | Technical Service Training for 2 to 8 Biomedical Engineering Technologists per session as described in Annex A, para 9.2 herein. | 1 | Session | $ | $ |
| | | | | **TOTAL OPTION REQUIREMENT - YEAR 2:** | **$** |

**2.3 OPTIONAL REQUIREMENT – YEAR 3: 01 APRIL 2026 TO 31 MARCH 2027**

| ITEM NO. | DESCRIPTION | QTY | UNIT OF ISSUE | UNIT RATE (CAD$) | EXTENDED RATE (CAD$) |
|---|---|---|---|---|---|
| | | (A) | | (B) | (C = A x B) |
| **1.0** | **EQUIPMENT** | | | | |
| 1.1 | Any type of probe-transmitter among -80 °C, -20°C, 2 °C to 8 °C, with its Certificate of Calibration testing, as referenced in Annex A, para 2.2.1.1 herein | Up to 24 | Each | $ | $ |
| 1.2 | Receiver-gateway fitted with Global System for Mobile communications (GSM) router, as referenced in Annex A, para 2.2.1.2 herein | Up to 6 | Each | $ | $ |
| 1.3 | Software package for one (1) additional probe-transmitter for one (1) year, as referenced in Annex A, para 2.2.3.1 herein | Up to 72 | Each | $ | $ |
| 1.4 | Cellular plan for one (1) additional receiver-gateway for one (1) year, as referenced in Annex A, para 2.2.3.3 herein | Up to 18 | Each | $ | $ |
| 1.5 | Software package for initial probes-transmitters as referenced in Annex A, para 2.2.3.2 herein | 1 | Each | $ | $ |
| 1.6 | Cellular network plan for initial receivers-gateways as referenced in Annex “A”, para 2.2.3.4 herein | 1 | Each | $ | $ |
| 1.7 | Offsite calibration of probes, as referenced Annex A, para 2.2.2.3 herein | 1 | Service | $ | $ |
| **2.0** | **TRAINING** | | | | |
| 2.1 | Virtual Operator Training Session for 5 to 10 operators per session as described in Annex A, para 9.1 herein. | Up to 10 | Session | $ | $ |
| 2.2 | Technical Service Training for 2 to 8 Biomedical Engineering Technologists per session as described in Annex A, para 9.2 herein. | 1 | Session | $ | $ |
| | | | | **TOTAL OPTION REQUIREMENT - YEAR 3** | **$** |

## 3.0 TOTAL EVALUATED PRICE (FOR BID EVALUATION PURPOSES ONLY)

| DESCRIPTION | TOTAL PRICE (CAD$) |
|---|---|
| Total Initial Contract Period | $_____ |
| Total Optional Requirement – Year 1 | $_____ |
| Total Optional Requirement – Year 2 | $_____ |
| Total Optional Requirement – Year 3 | $_____ |
| **TOTAL EVALUATED PRICE** | **$**_____ |

## ATTACHMENT 2 TO PART 3 - ELECTRONIC PAYMENT INSTRUMENTS

A. The Bidder accepts to be paid by any of the following Electronic Payment Instrument(s):

( ) VISA Acquisition Card;

( ) MasterCard Acquisition Card;

( ) Direct Deposit (Domestic and International); and

( ) Wire Transfer (International Only).

## PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

### 4.1 Evaluation Procedures

A. Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical criteria.

B. An evaluation team composed of representatives of Canada will evaluate the bids.

### 4.1.1 Technical Evaluation

#### 4.1.1.1 Mandatory Technical Criteria

A. Mandatory technical evaluation criteria are included in Attachment 1 to Part 4, Evaluation Criteria.

### 4.1.2 Financial Evaluation

A. The price of the bid will be evaluated as follows:

(i) Canadian-based bidders must submit firm prices, Canadian customs duties and excise taxes included, and Applicable Taxes excluded; and

(ii) Foreign-based bidders must submit firm prices, Canadian customs duties, excise taxes and Applicable Taxes excluded. Canadian customs duties and excise taxes payable by Canada will be added, for evaluation purposes only, to the prices submitted by foreign-based bidders.

B. Unless the bid solicitation specifically requires bids to be submitted in Canadian currency, bids submitted in foreign currency will be converted to Canadian currency for evaluation purposes. The rate given by the Bank of Canada in effect on the bid solicitation closing date, or on another date specified in the bid solicitation, will be applied as a conversion factor to the bids submitted in foreign currency.

C. Although Canada reserves the right to award the Contract either on an FOB plant or FOB destination, Canada requests that bidders provide prices FOB their plant or shipping point and FOB destination. Bids will be assessed on an FOB destination basis.

D. For the purpose of the bid solicitation, bidders with an address in Canada are considered Canadian-based bidders and bidders with an address outside of Canada are considered foreign-based bidders.

### 4.2 Basis of Selection - Lowest Evaluated Price, Mandatory Technical Criteria

A. A bid must comply with the requirements of the bid solicitation and meet all mandatory technical evaluation criteria to be declared responsive. The responsive bid with the lowest evaluated price will be recommended for award of a contract.

B. Should two (2) or more responsive bids achieve an identical lowest evaluated price, the bid that is received first, based on date and time will be recommended for award of a contract.

## ATTACHMENT 1 TO PART 4 - EVALUATION CRITERIA

A. A bid must comply with the requirements of the bid solicitation and meet all mandatory technical evaluation criteria to be declared responsive. The responsive bid with the lowest evaluated price will be recommended for award of a contract.

B. The following mandatory technical criteria must be demonstrated with supporting documentation in the form of a screen shot of equipment function from the equipment, user manual, technical/sales brochure, report and/or certifications which must be provided with the Bidder's response at the time of bid submission. Failure to submit supporting documentation that clearly demonstrates the mandatory technical criteria listed below, may render the bid non-compliant and will not be given further consideration. Any information proposed as options or additions to the work will NOT be evaluated.

### 1. Mandatory Technical Criteria

| # | MANDATORY TECHNICAL CRITERIA | BIDDER SUBSTANTIATION (INCLUDES LOCATION WITHIN PROPOSAL; TITLE, PAGE, ETC.) |
|---|---|---|
| **M1** | The Bidder must demonstrate that their proposed Environmental Monitoring Systems (EMS) have a Canadian Standards Association (CSA) certification (www.csagroup.org/global/en/about-csa-group/certification-marks-labels), or equivalency recognized by SCC (Standard Council of Canada) (www.scc.ca).<br><br>Proof of certification or proof of equivalency must be included with the bid submission. | |
| **M2** | The Bidder must demonstrate that that their proposed Environmental Monitoring Systems (EMS) are ready to transmit data to their web-based platform over cellular network and Ethernet.<br><br>In order to demonstrate M2, a reference in datasheet, brochure or manual must be included with the bid submission. | |
| **M3** | The Bidder must demonstrate that that their proposed Environmental Monitoring Systems (EMS) are capable of monitoring all of the following:<br>• Freezer temperature;<br>• Refrigerator temperature;<br>• Room temperature;<br>• Humidity;<br>• Power failure; and<br>• Flood | |

| | | |
|---|---|---|
| | A list of sensors compatible with the EMS devices must be included with the bid submission. | |
| **M4** | The Bidder must demonstrate that their proposed EMS software enables the creation of all of the following different user profiles:<br>• Administrator;<br>• Supervisor;<br>• User; and<br>• Quality Assurance.<br><br>Software screenshots showing the step by step the creation of different user profiles must be included with the bid submission. | |
| **M5** | The Bidder must demonstrate that their proposed EMS software has the capability to enable view, edit, add, and delete restrictions on each user profile on the following parameters:<br>• Device access; and<br>• User permission<br><br>Software screenshots showing the step by step the configuration of the EMS devices and permission restrictions on user profiles must be included with the bid submission. | |
| **M6** | For systems that use wireless probes-transmitters, the Bidder must demonstrate that the systems meet the Radio Standard Specifications of Innovation, Science and Economic Development Canada (ISED).<br><br>Proof of Technical Acceptance Certificate (TAC) must be included with bid submission. | |

## PART 5 - CERTIFICATIONS AND ADDITIONAL INFORMATION

A. Bidders must provide the required certifications and additional information to be awarded a contract.

B. The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

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

### 5.1 Certifications Required with the Bid

A. Bidders must submit the following duly completed certifications as part of their bid.

#### 5.1.1 Integrity Provisions - Declaration of Convicted Offences

A. In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide with their bid, **if applicable**, the Integrity 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 Contract Award and Additional Information

A. The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder 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 specified will render the bid non-responsive.

#### 5.2.1 Integrity Provisions - Required Documentation

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

#### 5.2.2 Security Requirements – Required Documentation

In accordance with the requirements of the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html), Canadian-based Bidders are required to provide a completed Contract Security Program Application for Registration (AFR) form, included in Attachment 1 to Part 5 to be given further consideration in the procurement process. Foreign-based Bidders are required to complete the Contract Security Program Initial International Security Screening (IISS) form, included in Attachment 2 to Part 5, to be given further consideration in the procurement process.

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

### 5.2.3 Federal Contractors Program for Employment Equity - Bid Certification

A. By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list available at the bottom of the page of the Employment and Social Development Canada (ESDC) - Labour's website (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html#).

B. Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the “FCP Limited Eligibility to Bid” list at the time of contract award.

**ATTACHMENT 1TO PART 5 – CONTRACT SECURITY PROGRAM (CSP) APPLICATION FOR REGISTRATION (AFR) FORM**

Bidders representing Canadian-based organizations are to complete the following AFR Form as part of their bid submission. If the AFR Form is not included as part of the bid submission, the Contracting Authority may request a copy prior to contract award:

Contract security program (CSP) - Application for registration (AFR) (pwgsc.gc.ca)

## ATTACHMENT 2 TO PART 5 – CONTRACT SECURITY PROGRAM (CSP) INITIAL INTERNATIONAL SECURITY SCREENING (IISS) FORM

Bidders representing foreign-based organizations are to complete the following IISS Form as part of their bid submission. If the IISS Form is not included as part of the bid submission, the Contracting Authority may request a copy prior to contract award:

**Purpose**

The purpose of this form is to initiate the security screening process for foreign suppliers who will need access to Canadian Protected/Classified information/assets/sites under a Government of Canada contract or Multinational Program processed by the Canadian Contract Security Program (CSP). The information provided may be disclosed to the Royal Canadian Mounted Police and Canadian Security Intelligence Service to conduct the requisite checks and/or investigation. Additionally, the information may be disclosed to and used by other Government of Canada institutions that may require this information as part of their functions or investigation under Canadian Law or for security assurances from foreign data protection authorities or industrial security programs of foreign governments.

The role of the Designated Security Authority for Canada (Canadian DSA) is performed by the International Industrial Security Directorate under the Contract Security Program and is the Canadian authority for confirming compliance with the Canadian national and international security requirements involving foreign suppliers.

### Instructions for completing this form

**General**

- This form and the additional documentation required must be provided in English or French.
- In any instance where this form does not allow enough space for a complete answer, please include additional pages and/or table rows as required.
- Refusal to provide the information, the provision of false statement, misleading information, or concealment and/or failure to disclose of any material fact on this screening form will result in a denial or revocation of eligibility to perform on contracts or multinational programs requiring access to Canadian Protected/Classified information/assets/sites.

**Section A - Business Information**

- You must provide all required documentation (outlined below) in relation to the type of company or corporate entity. Company or corporate entity's organization chart is mandatory for all types of entity.
- **Legal name of the company or corporate entity** refers to the legal name of the company or corporate entity as it is registered with the relevant foreign government authorities.
- **Business or trade name** refers to the name which a business trades under for commercial purposes, although its registered legal name used for contracts and other formal situations, may be another name.
- **Corporation** refers to an entity having authority under the law to act as a single person distinct from the shareholders who own it and having rights to issue stock and exist indefinitely. Provide the following additional information to substantiate this type of company or corporate entity selection:
    - Stock exchange identifier (if applicable); and
    - Certificate of Incorporation, compliance, continuance, etc.
- **Partnership** refers to a voluntary contract between two or more competent persons to place their money, effects, labor, and skill, or some or all of them, in lawful commerce or business, with the understanding that there shall be a proportional sharing of the profits and losses between them. Provide the following additional information to substantiate this type of company or corporate entity selection:

- Evidence of legal status (e.g. partnership documentation).

- **Sole proprietor** refers to the owner of a business who acts alone and has no partners. Provide the following additional information to substantiate this type of company or corporate entity selection:

  - Government registration documentation; and
  - Other (e.g. Master Business License).

- **State-owned entity** refers to a state-owned enterprise or government-owned enterprise where the government or state has significant control over this business entity through full, majority, or significant minority ownership. Provide the following additional information to substantiate this type of company or corporate entity selection:

  - National Law, Act or policies defining the entity; and
  - Evidence of legal status.

- **Other** (e.g. letters of patent, universities, financial institutions, unincorporated companies). Provide the following information to substantiate this type of company or corporate entity selection:

  - Evidence of legal status;
  - National laws and Acts; and/or
  - Charters.

- If the company or corporate entity is already registered in an industrial security program from the National Security Authority (NSA) or Designated Security Authority (DSA) of the relevant country, indicate the security level of its facility clearance and its date of validity.

- Indicate the name of the national Data Protection Authority (DPA) responsible for the protection of personal information in the country where the company or corporate entity is located and indicate the title of the legislation defining this authority.

**Section B – Company Security Officer (CSO)**

- Identify the individual that will be nominated as the company or corporate entity's Security Officer (hereinafter referred to as Company Security Officer (CSO)) who will be responsible for ensuring compliance with the security requirements of the Government of Canada contract or multinational program.

- The CSO **must** be:

  - an employee of the company or corporate entity; and
  - be security assessed at the same level as the company or corporate entity.

- The CSO must notify the Contract Security Program of any structure changes of the ownership for the company or corporate entity, including changes of the membership of its Board of Directors and the change of the nominated CSO.

- **Citizenship** refers to the status of being a citizen. A citizen is a person who, by either birth or naturalization, is a member of a political community, owing allegiance to the community and being entitled to enjoy all the civil rights and protections.

- For the purposes of the Contract Security Program, the term **Country of Primary Residence/National Domicile** refers to the particular country for a person's true, fixed, principal and permanent home, to which that person intends to return and remain even though currently residing elsewhere.

**Section C – List of Board of Directors**

- List all members of the company's Board of Directors. Applicants are to add additional rows to the section if required.

- **Citizenship** refers to the status of being a citizen. A citizen is a person who, by either birth or naturalization, is a member of a political community, owing allegiance to the community and being entitled to enjoy all the civil rights and protections.

- For the purposes of the Contract Security Program, the term **Country of Primary Residence/National Domicile** refers to the particular country for a person's true, fixed, principal and permanent home, to which that person intends to return and remain even though currently residing elsewhere.

**Section D - Ownership Information**

- For the purposes of the Contract Security Program, the following interpretations are applicable:

    - **Direct (or registered)** owners are owners who hold legal title to a property or asset in that owner's name.
    - **Ownership** refers to either (1) voting rights attached to the corporation's outstanding voting shares or (2) outstanding shares measured by fair market value.

- **Parent company or corporate entity** refers to a company or corporate entity which owns and/or controls controlling interest (e.g. voting stock) of other firms or companies, usually known as subsidiaries, which may give it control of the operation of the subsidiaries.

**Section E - Certification and Consent**

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

**IMPORTANT NOTE:** The provision of false, misleading information, or concealment and/or failure to disclose of any material fact on this screening form will prohibit your eligibility to perform on contracts or multinational programs requiring access to Canadian Protected/Classified information/assets/sites. An incomplete form will not be processed by the Contract Security Program and will be returned to you.

| **SECTION A - BUSINESS INFORMATION** |
|---|
| **Complete Section A and provide the required documentation identified in the instructions above.** |
| 1. Legal name of the company or corporate entity |
| 2. Business or trade name (if different from legal name) |
| 3. Type of company or corporate entity (Indicate the type of organization and provide the required validation documentation)<br>(select one only)<br>☐ Sole proprietor<br>☐ Partnership<br>☐ Corporation (Private or Public)<br>☐ State-owned entity<br>☐ Other, specify: |

| | | |
|---|---|---|
| 4. Provide a brief description of your company or corporate entity's general business activities | | |
| 5. Business (Head office) civic address | | |
| 6. Mailing address (if different from business civic address) | | |
| 7. Company or corporate website (if applicable) | | |
| 8. Business Identifier Number if applicable (e.g. CAGE/NCAGE code) | 9. Telephone number (include country code and extension number if any) | 10. Facsimile number if applicable (include country code) |
| 11. Number of employees in your company or corporate entity | | 12. Number of employees who require access to Canadian Protected/Classified information/assets/sites |
| 13. Indicate the valid facility security level of the company or corporate entity granted by the relevant National Security Authority or Designated Security Authority (indicate NIL if none) | | 14. Provide the date of the validity of the facility clearance (if applicable) |
| 15. Name of the relevant national Data Protection Authority (DPA) responsible for the protection of personal information in the country (indicate NIL if none) | | 16. Title of the legislation defining the Data Protection Authority (DPA) (if applicable) |

| **SECTION B – COMPANY SECURITY OFFICER** | | | | |
|---|---|---|---|---|
| **Complete Section B.** | | | | |
| Position title | Surname | Given name(s) | Citizenship(s) | Country of primary residence/National domicile |
| | | | | |
| Email address for the company security officer: | | | | |

| **SECTION C – LIST OF MEMBERS OF THE BOARD OF DIRECTORS (INDICATE N/A IF NOT APPLICABLE)** | | | | |
|---|---|---|---|---|
| **Complete Section C. Add additional rows or attachment as required** | | | | |
| Position title | Surname | Given name(s) | Citizenship(s) | Country of primary residence/National domicile |
| | | | | |
| | | | | |
| | | | | |

| **SECTION D – OWNERSHIP INFORMATION** | | | | | |
|---|---|---|---|---|---|
| **Complete Section D for each level of ownership**<br>Identify all entities, individuals, public or private corporations that have an ownership stake in the organization listed in Section 1. For publicly traded corporations, identify stock exchange. An ownership relation chart with percentages of ownership must be included. | | | | | |
| **SECTION D-1 – OWNERSHIP LEVEL 1 (DIRECT OWNERSHIP)** | | | | | |
| Identify all individual owners or direct organizations ownership related to the company or corporate entity identified in | | | | | |
| Name of organization or individual | Address | Type of entity (e.g. private or public corporation, state-owned) | Stock exchange (public or private) | Percentage of ownership | Country of jurisdiction or citizenship |
| | | | | | |
| | | | | | |
| | | | | | |
| **SECTION D-2 – OWNERSHIP LEVEL 2** | | | | | |
| If there is any additional ownership for the names listed in the previous section (D-1), provide the information below. If none, please indicate N/A (not applicable). | | | | | |
| Name of organization or individual | Address | Type of entity (e.g. private or public corporation, state-owned) | Stock exchange (public or private) | Percentage of ownership | Country of jurisdiction or citizenship |
| | | | | | |
| | | | | | |
| | | | | | |
| **SECTION D-3 – OWNERSHIP LEVEL 3** | | | | | |
| If there is any additional ownership for the names listed in the previous section (D-2) please provide the information below. If none, please indicate N/A (not applicable). | | | | | |
| Name of organization or individual | Address | Type of entity (e.g. private or public corporation, state-owned) | Stock exchange (public or private) | Percentage of ownership | Country of jurisdiction or citizenship |
| | | | | | |
| | | | | | |
| | | | | | |

| **SECTION E – CERTIFICATION AND CONSENT (only an individual identified in Section C may complete this section)** | |
|---|---|
| I, the undersigned, as the individual authorized by the organization identified in Section 1, have read the purpose and instructions of this screening form and do hereby certify that the information contained in this screening form is true, complete and correct. I acknowledge and agree to comply with the responsibilities outlined in the Public Services and Procurement Canada's Contract Security Manual and consent to the collection, use and disclosure of the information provided in this screening form for the purposes as described above. I agree to notify the Contract Security Program of any changes to the organization such as change of address, contact phone numbers, email address, change in company management structure, ownership, company security officer and the members of the Board of Directors. | |
| Surname | Given name(s) |
| Position title | Telephone number (include country code and extension number if any) |

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

| Facsimile number if applicable (include country code) | Email address |
|---|---|
| Signature | Date |

| **FOR USE BY THE PSPC'S CONTRACT SECURITY PROGRAM** | | |
|---|---|---|
| Recommendations | | |
| Recommendation by analyst (Name) | Signature | Date |
| Approval (Name) | Signature | Date |

## PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

### 6.1 Security Requirements

1. Before award of a contract, the following conditions must be met:

   (a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

   (b) the Bidder must provide the addresses of proposed sites or premises of work performance and document safeguarding as indicated in Part 3 - Section IV Additional Information.

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

   (a) the Bidder's proposed individuals requiring access to sensitive information, assets or sensitive work sites must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses.

   (b) the Bidder's security capabilities must be met as indicated in Part 7 - Resulting Contract Clauses;

3. For additional information on security requirements, Bidders 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.

## PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

### ARTICLES OF AGREEMENT

#### 7.1 Statement of Requirement

A. The Contractor must provide the items detailed under the Statement of Requirement at Annex A.

#### 7.2 Standard Clauses and Conditions

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

#### 7.2.1 General Conditions

A. 2030 (2022-05-12), General Conditions - Goods (High Complexity), apply to and form part of the Contract, with the following modification:

(i) Article 01, Interpretation, "Canada", "Crown", "Her Majesty" or "the Government", is deleted in its entirety and replaced with the following:

"Canada", "Crown", "Her Majesty" or "the Government"
means Her Majesty the Queen in right of Canada as represented by the Minister of National Defence and any other person duly authorized to act on behalf of that minister or, if applicable, an appropriate minister to whom the Minister of National Defence has delegated his or her powers, duties or functions and any other person duly authorized to act on behalf of that minister.

B. 2035 (2022-05-12), General Conditions: Higher Complexity - Services, apply to and form part of the Contract, with the following modification:
The General Conditions

(i) Article 01, Interpretation, "Canada", "Crown", "Her Majesty" or "the Government", is deleted in its entirety and replaced with the following:

"Canada", "Crown", "Her Majesty" or "the Government"
means Her Majesty the Queen in right of Canada as represented by the Minister of National Defence and any other person duly authorized to act on behalf of that minister or, if applicable, an appropriate minister to whom the Minister of National Defence has delegated his or her powers, duties or functions and any other person duly authorized to act on behalf of that minister.

#### 7.2.2 Supplemental General Conditions

A. The following Supplemental General Conditions apply to and form part of the Contract:

(i) 4001 (2015-04-01), Hardware Purchase, Lease and Maintenance;

(ii) 4003 (2010-08-16), Licensed Software;

(iii) 4004 (2013-04-25), Maintenance and Support Services for Licensed Software;

(iv) 4006 (2010-08-16), Contractor to Own Intellectual Property Rights in Foreground Information;

**7.3 Security Requirements**

A. The following security requirements apply and form part of the Contract:

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

(ii) The Contractor/Offeror personnel requiring access to PROTECTED information, assets or sensitive site(s) must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required by the security guide, granted or approved by the CSP, PWGSC.

(iii) The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until written approval has been issued by the client department security authority. After approval has been granted, these tasks may be performed at the level of PROTECTED A.

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

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

(a) Security Requirements Check List and security guide, attached at Annex C;
(b) Contract Security Manual (Latest Edition);
(c) CSP website: Security requirements for contracting with the Government of Canada, located at www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html

**7.3.1 Contractor's Sites or Premises Requiring Safeguarding Measures**

A. Where safeguarding measures are required in the performance of the Work, the Contractor must diligently maintain up-to-date the information related to the Contractor's and proposed individuals' sites or premises for the following addresses:

[Location(s) to be detailed in the resulting contract]

B. The Company Security Officer must ensure through the Contract Security Program (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) that the Contractor and individuals hold a valid security clearance at the required level.

**7.4 Term of Contract**

**7.4.1 Period of the Contract**

A. The period of the Contract is from date of Contract is awarded to 31 March 2027, inclusive.

**7.4.2 Delivery Date**

A. All deliverables for the Initial Contract Period must be received on or before 30 August 2023. All deliverables for the Optional Requirement, needed on an "as and when required" basis, must be delivered before 31 March 2027.

**7.4.3 Delivery Points**

A. Delivery of the requirement will be made to delivery point specified at Annex A, Statement of Requirement, of the Contract.

**7.5 Authorities**

**7.5.1 Contracting Authority**

A. The Contracting Authority for the Contract is:

Name: Lana Ibrahim
Title: Senior Procurement Officer, D Svcs C 3-4-2
Organization: Director Services Contracting 3 (D Svcs C 3)
Address: Department of National Defence
101 Colonel By Drive
Ottawa ON K1A 0K2
E-mail: Lana.Ibrahim@forces.gc.ca

B. The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

**7.5.2 Technical Authority**

A. The Technical Authority for the Contract is:

[Contact information to be detailed in the resulting contract]
Name: _____
Title: _____
Organization: _____
Address: Department of National Defence (DND)
101 Colonel By Drive
Ottawa ON K1A 0K2
Telephone: _____
E-mail: _____

B. The Technical Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of

the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

### 7.5.3 Contractor's Representative

[Contact information to be detailed in the resulting contract]
Name: _____
Title: _____
Address: _____
_____
_____
Telephone: _____
E-mail: _____

## 7.6 Payment

### 7.6.1 Basis of Payment - Firm Price

A. In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid a firm price as specified in Annex B, Basis of Payment, for the cost of _____$ (amount to be detailed in the resulting contract). Customs duties are excluded and Applicable Taxes are extra.

B. Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work, unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

### 7.6.2 Limitation of Price

A. Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

### 7.6.3 Method of Payment - Multiple Payments

A. Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Contract if:

i. an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

ii. all such documents have been verified by Canada;

iii. the Work delivered has been accepted by Canada

### 7.6.4 Taxes - Foreign-based Contractor

A. Unless specified otherwise in the Contract, the price includes no amount for any federal excise tax, state or local sales or use tax, or any other tax of a similar nature, or any Canadian tax whatsoever. The price, however, includes all other taxes. If the Work is normally subject to federal excise tax, Canada will, upon request, provide the Contractor a certificate of exemption from such federal excise tax in the form prescribed by the federal regulations.

B Canada will provide the Contractor evidence of export that may be requested by the tax authorities. If, as a result of Canada's failure to do so, the Contractor has to pay federal excise tax, Canada will reimburse the Contractor if the Contractor takes such steps as Canada may require to recover any payment made by the Contractor. The Contractor must refund to Canada any amount so recovered.

**7.6.5. SACC Manual Clauses**

A. C2608C (2020-07-01), Canadian Customs Documentation

B. C2610C (2007-11-30), Customs Duties - Department of National Defence – Importer

**7.6.6 Electronic Payment of Invoices - Contract**

A. The Contractor accepts to be paid using any of the following Electronic Payment Instrument(s):

[List to be updated in the resulting contract]

(i) Visa Acquisition Card;

(ii) MasterCard Acquisition Card;

(iii) Direct Deposit (Domestic and International); and

(iv) Wire Transfer (International Only).

**7.7 Invoicing Instructions**

A. The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. Invoices cannot be submitted until all work identified in the invoice is completed.

B. Each invoice must be supported by:

(i) A copy of the release document and any other documents as specified in the Contract;

(ii) A description of the Work delivered; and

(iii) A breakdown of the cost elements.

C. Invoices must be distributed as follows:

(i) The original and one (1) copy must be forwarded to the address shown on page 1 of the Contract for certification and payment.

(ii) One (1) copy must be forwarded to the Contracting Authority identified under the section entitled "Authorities" of the Contract.

### 7.8 Certifications and Additional Information

#### 7.8.1 Compliance

A. Unless specified otherwise, the continuous compliance with the certifications provided by the Contractor in its bid or precedent to contract award, and the ongoing cooperation in providing additional information are conditions of the Contract and failure to comply will constitute the Contractor in default. Certifications are subject to verification by Canada during the entire period of the Contract.

### 7.9 Applicable Laws

A. The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario [or as specified by the bidder in its bid, if applicable].

### 7.10 Priority of Documents

A. 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:

(i) The Articles of Agreement;

(ii) The Supplemental General Conditions:
a) 4001 (2015-04-01), Hardware Purchase, Lease and Maintenance;
b) 4003 (2010-08-16), Licensed Software;
c) 4004 (2013-04-25), Maintenance and Support Services for Licensed Software;
d) 4006 (2010-08-16), Contractor to Own Intellectual Property Rights in Foreground Information;

(iii) The General Conditions 2030 (2022-05-12), General Conditions – Higher Complexity Goods

(iv) The General Conditions 2035 (2022-05-12), General Conditions - Higher Complexity - Services;

(v) Annex A, Statement of Requirement;

(vi) Annex B, Basis of Payment;

(vii) Annex C, Security Requirements Check List;

(viii) The Contractor's bid dated [date to be specified in the resulting contract], as clarified on [date to be specified in the resulting contract, if required], and as amended on [date to be specified in the resulting contract, if required].

### 7.11 Defence Contract

A. The Contract is a defence contract within the meaning of the *Defence Production Act*, R.S.C. 1985, c. D-1 (https://laws-lois.justice.gc.ca/eng/acts/d-1/) and must be governed accordingly.

B. Title to the Work or to any materials, parts, work-in-process or finished work must belong to Canada free and clear of all claims, liens, attachments, charges or encumbrances. Canada is entitled, at any time, to remove, sell or dispose of the Work or any part of the Work in accordance with section 20 of the *Defence Production Act*.

**7.12 Excess Goods**

A. The quantity of goods to be delivered by the Contractor is specified in the Contract. The Contractor remains liable for any shipment in excess of that quantity whether the excess quantity is shipped voluntarily or as a result of an error by the Contractor. Canada will not make any payment to the Contractor for goods shipped in excess of the specified quantity. Canada will not return the said goods to the Contractor unless the Contractor agrees to pay for all the costs related to the return, including but not limited to administrative, shipping and handling costs. Canada will have the right to deduct such costs from any invoice submitted by the Contractor.

**7.13 Canadian Forces Site Regulations**

A. The Contractor must comply with all standing orders or other regulations, instructions and directives in force on the site where the Work is performed.

**7.14 Delivery and Unloading**

A. Delivery trucks must be equipped with an unloading device which will permit unloading at sites with no hydraulic, stationary or other type of unloading facility.

B. When making deliveries, sufficient personnel must be provided to permit unloading of any type of vehicle without the assistance of federal government personnel.

C. At some sites, the delivery truck must be unloaded while parked at the curb. When material is placed on the sidewalk, it must be placed in proximity to the designated entrance so as to be readily accessible to transport by mechanical handling equipment utilized by site personnel.

**7.15 Marking**

A. The Contractor must ensure that the manufacturer's name and part number are clearly stamped or etched on each item for positive identification purposes.

**7.16 Labelling**

A. The Contractor must ensure that the manufacturer's and specification numbers appear on each item, either printed on the container or on an adhesive label of highest commercial standard affixed to the container.

**7.17 Palletization**

A. For all shipments exceeding 0.566 m3 or 15.88 kg (20 ft3 or 35 lbs), except for those shipped by courier, the following applies:

(i) The Contractor must strap, and if necessary wrap, shipments on standard 1.22 m x 1.02 m (48 in. x 40 in.) wood pallets. The four-way forklift entry pallet must be supplied at no charge to Department of National Defence. Total height, including pallet, must not exceed 1.19 m

(47 in.). The pallet load must not extend further than 2.54 cm (1 in.) from any edge of the pallet.

(ii) The Contractor must group items by stock number (on the same pallet) within consolidated shipments. Pallet loads composed of more than one stock number must be marked as "Mixed Items".

(iii) Individual items exceeding 1.22 m (48 in.) in length or 453.6 kg (1000 lbs) must be secured to larger pallets or must have 10.16 cm x 10.16 cm (4 in. x 4 in.) skids securely fastened to the bottom of the item. Skids must be separated by a minimum of 71.12 cm (28 in.).

B. Any exception requires the prior approval of the Contracting Authority.

One (1) of the following two (2) options will be inserted in the resulting contract, as applicable:

Option 1: A2000C (2006-06-16) when the contract is to be with a Canadian-based supplier; or

**7.18 Foreign Nationals (Canadian Contractor)**

A. The Contractor must comply with Canadian immigration requirements applicable to foreign nationals entering Canada to work temporarily in fulfillment of the Contract. If the Contractor wishes to hire a foreign national to work in Canada to fulfill the Contract, the Contractor should immediately contact the nearest Service Canada regional office to enquire about Citizenship and Immigration Canada's requirements to issue a temporary work permit to a foreign national. The Contractor is responsible for all costs incurred as a result of non-compliance with immigration requirements.

Option 2: A2001C (2006-06-16) when the contract is to be with a foreign-based supplier.

**7.18 Foreign Nationals (Foreign Contractor)**

A. The Contractor must comply with Canadian immigration legislation applicable to foreign nationals entering Canada to work temporarily in fulfillment of the Contract. If the Contractor wishes to hire a foreign national to work in Canada to fulfill the Contract, the Contractor should immediately contact the nearest Canadian Embassy, Consulate or High Commission in the Contractor's country to obtain instructions, information on Citizenship and Immigration Canada's requirements and any required documents. The Contractor is responsible to ensure that foreign nationals have the required information, documents and authorizations before performing any work under the Contract in Canada. The Contractor is responsible for all costs incurred as a result of non-compliance with immigration requirements.

**7.19 Insurance-No Specific Requirement**

A. The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection. It does not release the Contractor from or reduce its liability under the Contract.

**7.20 Shipping Instruction (DND) – Delivered at Place (DAP) Incoterm 2010**

A. Goods must be shipped DAP – Delivered at Place to the delivery location mentioned in Annex A. The Contractor is responsible for export clearance, delivery charges, administration, costs and risks of transport. DND is responsible for all import clearance, including the payment of applicable duties and taxes.

### 7.21 Dispute Resolution

(A) The parties agree to maintain open and honest communication about the Work throughout and after the performance of the contract.

(B) The parties agree to consult and co-operate with each other in the furtherance of the contract and promptly notify the other party or parties and attempt to resolve problems or differences that may arise.

(C) If the parties cannot resolve a dispute through consultation and cooperation, the parties agree to consult a neutral third party offering alternative dispute resolution services to attempt to address the dispute.

(D) Options of alternative dispute resolution services can be found on Canada's Buy and Sell website under the heading "Dispute Resolution".

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

## ANNEX A - STATEMENT OF REQUIREMENT

## ENVIRONMENTAL MONITORING SYSTEM (EMS)

### 1. INTRODUCTION

1.1 The Department of National Defence (DND) has a requirement for the supply of Environmental Monitoring Systems (EMS) fitted with data loggers and alarms to continuously and remotely monitor the temperature of 2$^{o}$C to 8$^{o}$C refrigerators as well as -20$^{o}$C and -80$^{o}$C freezers deployed for the storage of COVID-19 vaccines.

### 2. GOODS AND SERVICES

2.1 Initial (core) requirement:

The Contractor must provide a solution to monitor, from a central web-based platform, the temperature of ninety six (96) refrigerators and freezers located in thirty (30) different sites across Canada (see

APPENDIX 1 TO ANNEX A - LOCATIONS OF ASSETS TO MONITOR).

*2.1.1. Equipment*

2.1.1.1 Probes-transmitters with Certificate of Calibration testing:
2.1.1.1.1 Five (5) for -80ºC freezers
2.1.1.1.2 Thirty (30) for -20ºC freezers
2.1.1.1.3 Sixty one (61) for 2ºC to 8ºC refrigerators

2.1.1.2 Receivers-gateways fitted with Global System for Mobile communications (GSM) router. The total quantity of receivers-gateways must be determined by the Contractor based on the technology submitted and the layout of the refrigerators and freezers per location (see APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION). The Contractor must indicate the number of receiver-gateways required for each location.

*2.1.2 Subscription (recurring)*

2.1.2.1 Software package for ninety six (96) probes-transmitters, with unlimited number of users and unlimited alarms (phone, e-mail, or text).
2.1.2.2 Cellular network plan for each receiver-gateway with enough data to support 10 probes at 5 minute sampling interval.

2.1.3 *Services*

2.1.3.1 One (1) Operator Training session per site, for 5 to 10 people
2.1.3.2 One (1) Technical Training for 2 to 8 people

2.2 Optional Requirement:

*2.1.2 Equipment*

2.1.2.1 Additional probes-transmitters with their Certificate of Calibration testing, up to 72 units over 3 years (i.e., up to 24 units each year)
2.1.2.2 Additional receivers-gateways fitted with GSM router, up to 18 units over 3 years (i.e., up to 6 units each year)

2.2.2 *Services*

2.2.2.1 One (1) Operator Training session per site, for 5 to 10 people
2.2.2.2 One (1) Technical Training for 2 to 8 people
2.2.2.3 One (1) Offsite Calibration of Probes per year, up to 3 years

2.2.3 *Subscription (recurring)*

2.2.3.1 Additional probes on software package, up to 72 units over 3 years (i.e., up to 24 units each year). Additional years on software package subscription, up to 3 years
2.2.3.2 Additional cellular network plans, up to 18 over 3 years (i.e., up to 6 each year,)
2.2.3.3 Additional years on cellular network plans, up to 3 years

**3. CERTIFICATIONS AND STANDARDS**

3.1 The Environmental Monitoring Systems (EMS) must have a Canadian Standards Association (CSA) certification, or equivalent (proof of certification or proof of equivalency must be included with the bid submission) (www.csagroup.org/global/en/about-csa-group/certification-marks-labels. Equivalency must be recognized by SCC (Standard Council of Canada) (www.scc.ca).

3.2 The Environmental Monitoring Systems (EMS) must have a validated software: Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ)

3.3 The Environmental Monitoring Systems (EMS) must have a software compliant with the Food and Drug Administration's (FDA's) part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures (21 CFR Part 11).

3.4 The probes of the Environmental Monitoring Systems (EMS) must have a National Institute of Standards and Technology (NIST) traceable 3-point Certificate of Calibration Testing with a guaranteed error of no more than ± 0.5C at each calibration point

**4. HARDWARE REQUIREMENTS**

4.1 The environmental monitoring system must be capable of monitoring:

4.1.1. Freezer temperature;
4.1.2. Refrigerator temperature;
4.1.3. Room temperature;
4.1.4. Humidity;
4.1.5. Power failure; and
4.1.6. Flood.

4.2 The Environmental Monitoring Systems (EMS) must be capable of measuring temperature ranges from -86°C to 10°C.

4.3 The probes of the Environmental Monitoring Systems (EMS) must have an uncertainty of +/-0.5°C (+/-1° F).

4.4 The Environmental Monitoring Systems (EMS) must have real time data collection and real time data transfer to a secured central web-based platform (software). The delay between present temperature and reported temperature in the software must be no more than 1 hour.

4.5 The Environmental Monitoring Systems (EMS) of the thirty (30) sites must be connected on the same software.

4.6 The Environmental Monitoring Systems (EMS) must be ready to transmit data to the web-based platform (software) over cellular network and Ethernet.

4.7 The Environmental Monitoring Systems (EMS) must include a secured portal for remote access to the data collected.

4.8 The Environmental Monitoring Systems (EMS) must include audible and visible alarms for each freezer and refrigerator.

4.9 The Environmental Monitoring Systems (EMS) must be capable of accommodating additional sensors after it is implemented.

4.10 The Environmental Monitoring Systems (EMS) must be capable of being re-located for future extension or installation in different locations, while allowing data access through the same software

4.11 The Environmental Monitoring Systems (EMS) must have a battery backup.

**5. SOFTWARE REQUIREMENTS**

5.1 The software must be capable of supporting a large number of sensors on the same database, for extension purposes (more than 1000).

5.2 The software must enable assigning a location and identifier to each device.

5.3 The software must be accessible from mobile devices or personal computers.

5.4 The software must be accessible by minimum 100,000 users. The user access must be at the discretion of DND.

5.5 The software must support user authentication with a personal user ID and password.

5.6 The software must enable the creation of different user profiles:

5.6.1 Administrator;
5.6.2 Supervisor;
5.6.3 User; and
5.6.4 Quality assurance.

5.7 The software must enable view, edit, add, and delete restrictions on each user profile on the following parameters:

5.7.1 Device access; and
5.7.2 User permissions

5.8 The software must allow for the complete remote configuration of the devices including the following:

5.8.1 Sampling intervals;
5.8.2 Temperature limits;
5.8.3 Alarms setups; and
5.8.4 Reports configuration

5.9 The software must allow tiered alarm management including:

5.9.1 Unlimited number of alarms to be sent by text message, phone, e-mail;
5.9.2 Alarms to be sent to up to 4 separate points of contact; and
5.9.3 Alarms must have a configurable frequency for sending alerts which have not been responded to

5.10 The software must allow sampling intervals of no less t 5 minutes.

5.11 The software must have a minimum of 12 months of data storage capacity for reporting

5.12 The software must provide data history for each sensor. Data must be available for export into Microsoft Excel.

5.13 The software must provide automated reports on daily, weekly, monthly basis (each sensor separately) and as a table containing all sensors min and max values.

5.14 The software must generate reports that cannot be edited.

## 6. IT REQUIREMENTS

6.1 Wireless probes-transmitters

6.1.1 For systems that use wireless probes-transmitters, they must:

6.1.1.1 Meet the Radio Standard Specifications of Innovation, Science and Economic Development Canada (ISED). The Contractor must provide a proof of Technical Acceptance Certificate (TAC);
6.1.1.2 Have a wireless range less than 30 meters for security purposes; and
6.1.1.3 Provide a general description of their intended spectrum usage: intended frequency bands, number of channels required, approximate transmitting power, and approximate bandwidth requirements. The use of diagrams to facilitate system operation understanding is required.

6.1.2 Web-based platform security:
6.1.2.1 The data must be processed in an Operation Zone;
6.1.2.2 The software must include a security audit log function to enable the detection of incidents; and
6.1.2.3 The software must comply with minimum standard that is Advanced Encryption Standard 128 (AES-128) and Transport Layer Security 1.2 (TLS 1.2).

## 7. DELIVERY

7.1 The Contractor must deliver the goods to the following address:

Central Medical Equipment Depot (CMED)
105 Montgomery road, BB 104-A
Petawawa, ON
K8H 2X3
Canada

## 8. INSTALLATION

8.1 The Contractor must provide technical support to the DND Biomedical Engineering Technologist personnel in order to perform the installation.

8.2 The activation of the subscriptions must not start before the installation date.

## 9. TRAINING

### 9.1 OPERATOR TRAINING

9.1.1 At the client's request, the Contractor must provide virtual Operator Training course for DND personnel. At a minimum, the training course must provide DND personnel with the knowledge necessary to navigate the various menus, systems and sub-systems, including basic troubleshooting of the system. At the completion of the training, Canadian Forces Health Services personnel must be comfortable operating the system.

9.1.2 The Contractor must provide:

9.1.2.1 *Sessions:* Upon request by DND, 1 mandatory and 1 optional Operator Training session per DND locations identified in APPENDIX 1 TO ANNEX A - LOCATIONS OF ASSETS TO MONITOR, as referenced in sections 0 and 0. Each session must be for an estimated 5 -10 personnel;

9.1.2.2 *Timeline:* the training must be completed within 60 calendar days of the system delivery or as soon as possible at a date and time agreed upon between the Contractor's representative and the Technical Authority.

9.1.2.3 *Location:* The training is to be provided by live webinar for DND locations identified in APPENDIX 1 TO ANNEX A - LOCATIONS OF ASSETS TO MONITOR. The Contractor's representative will provide a link or recording of this training for use by the CAF in future trainings to the Technical Authority.

9.1.2.4 *Language:* Training must be provided in both French and English upon agreement between the Contractor's representative and the Technical Authority as to which webinar will be offered in each location as specified in APPENDIX 1 TO ANNEX A - LOCATIONS OF ASSETS TO MONITOR.

9.1.2.5 *License:* the Contractor grants a perpetual, non-revocable license to use, reproduce, and translate the training and reference manuals, materials and documentation.

9.1.2.6 *Documentation:* the Contractor must provide, at a minimum, 1 hardcopy and 1 soft copy in PDF format of the Operator Training course manual for each participant on the first day of the course. The Operator Training course manual must be available in English and in French. The Technical Authority will provide the Contractor with a list of attendees no later than 5 days prior to the start of the course.

## 9.2 TECHNICAL TRAINING

9.2.1 The Contractor must provide, hands-on Technical Service training course for DND Biomedical Engineering Technologist personnel. The Technical Service training provided must be to the same level and extent as that which the Original Equipment Manufacturer (OEM) provides to its field service engineers. At the completion of the training, DND Biomedical Engineering Technologist personnel must be comfortable diagnosing, troubleshooting, repairing, and operating the system. At a minimum, the Technical Service training course must provide DND Biomedical Engineering Technologist personnel with the knowledge necessary to efficiently navigate the various menus, systems, and sub-systems, the comprehensive training on repair, calibration, and system troubleshooting and its peripherals.

9.2.2 The Contractor must provide:

9.2.2.1 *Sessions:* Upon request by DND, 1 mandatory and 1 optional Technical Service training session, as referenced in sections 0 and 0, at the same level and extent as the Original Equipment Manufacturer (OEM) provides to its field service engineers. Each Technical Service training session will be for a group estimated at between 2 to 8 Biomedical Engineering Technologists.

9.2.2.2 *Timeline:* the training must be completed within 60 calendar days of the system delivery or as soon as possible at a date and time agreed upon between the Contractor's representative and the Technical Authority.

9.2.2.3 *Location:* The training will take place at Central Medical Equipment Depot (CMED) Petawawa (refer to 7.1 for full address). The Contractor's course fees will be all-inclusive of travel and accommodation expenses.

9.2.2.4 *Language:* must be performed in English.

9.2.2.5 *License:* the Contractor grants a perpetual, non-revocable license to use, reproduce, and translate the training and reference manuals, materials and documentation.

9.2.2.6 *Documentation*: the Contractor must provide 1 copy of the technical/service manual, with schematics and list of replacement parts, for each participant on the first day of the course. The Technical Authority will provide the Contractor with a list of Biomedical Engineering Technologist attendees no later than 5 days prior to the start of the course.

## 10. ACCEPTANCE TESTING

10.1 DND acceptance of the solution will be contingent upon the successful completion of testing of a representative sample of the solution at one of the DND sites: Halifax. The Contractor must provide the devices, software, and all other parts of the solution that would be required for Halifax. The representative sample of the solution will be tested in accordance with the requirements specified in sections 4 and 5 of this SOR post installation as referenced in APPENDIX 2 TO ANNEX A – ENVIRONMENTAL MONITORING SYSTEM – ACCEPTANCE TESTING CHECKLIST.

10.2 To assist with the acceptance testing, the Contractor must provide, at no additional cost to DND, personnel to answer any technical questions on the hardware and software which may arise during the testing.

10.3 Upon completion of the acceptance testing, DND will provide the Contractor with a copy of the acceptance testing results. The Contractor will be responsible for correcting any issues identified at no additional cost to DND.

## 11. TECHNICAL SUPPORT

11.1 The Contractor must provide technical support via telephone, available from Monday to Friday 8am to 5pm, local time at all locations identified in

APPENDIX 1 TO ANNEX A - LOCATIONS OF ASSETS TO MONITOR - LOCATIONS OF ASSETS TO MONITOR.

11.2 The Contractor must provide an optional annual calibration service of probes offsite as referenced in section 0. A rotation service must be available in the locations specified at APPENDIX 1 TO ANNEX A – LOCATIONS OF ASSETS TO MONITOR.

.

## APPENDIX 1 TO ANNEX A - LOCATIONS OF ASSETS TO MONITOR

| Province | Location | Freezer -80 | Freezer -20 | Refrigerator | Layout |
|---|---|---|---|---|---|
| Alberta | Cold Lake | | 1 | 3 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Alberta | Edmonton | 1 | 1 | 2 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Alberta | Suffield | | 1 | 1 | Freezer and refrigerator co-located in the same room |
| Alberta | Wainright | | 1 | 2 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| British Columbia | Comox | | 1 | 1 | Freezer and refrigerator co-located in the same room two (2) feet from one another. |
| British Columbia | Esquilmat | 1 | 1 | 3 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| British Columbia | Vancouver | | 1 | 1 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Manitoba | Shilo | | 1 | 4 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Manitoba | Winnipeg | | 1 | 2 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| New Brunswick | Gagetown | | 1 | 3 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Newfoundland & Labrador | Gander | | 1 | 1 | Freezer and refrigerator co-located in the same room |
| Newfoundland & Labrador | Goose Bay | | 1 | 1 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Newfoundland & Labrador | St-John's | | 1 | 1 | APPENDIX 3 TO ANNEX A - LAYOUT OF |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | REFRIGERATORS AND FREEZERS PER LOCATION |
| North | Yellow Knife | | 1 | 1 | Freezer and refrigerator co-located in the same room |
| Nova Scotia | Greenwood | | 1 | 1 | Freezer and refrigerator co-located in the same room |
| Nova Scotia | Halifax | 1 | 1 | 1 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Ontario | Borden | | 1 | 3 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Ontario | Kingston | | 1 | 6 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Ontario | Meaford | | 1 | 2 | Freezer and refrigerators co-located in the same room |
| Ontario | North Bay | | 1 | 1 | Freezer and refrigerator co-located in the same room |
| Ontario | Ottawa | | 1 | 6 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Ontario | Petawawa | | 1 | 1 | Freezer and refrigerator co-located one (1) feet apart |
| Ontario | Toronto | | 1 | 1 | Freezer and refrigerator co-located in the same room |
| Ontario | Trenton | | 1 | 4 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Quebec | Bagotville | | 1 | 1 | Freezer and refrigerator co-located in the same room |
| Quebec | Montreal | | 1 | 2 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Quebec | St-Jean | 1 | 1 | 3 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Quebec | Valcartier | 1 | 1 | 1 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |
| Saskatchewan | Dundurn | | 1 | 1 | APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION |

| | | | | | |
|---|---|---|---|---|---|
| Saskatchewan | Moose Jaw | | 1 | 1 | Freezer and refrigerator co-located in the same room five (5) feet apart |
| | **TOTAL** | **5** | **30** | **61** | |

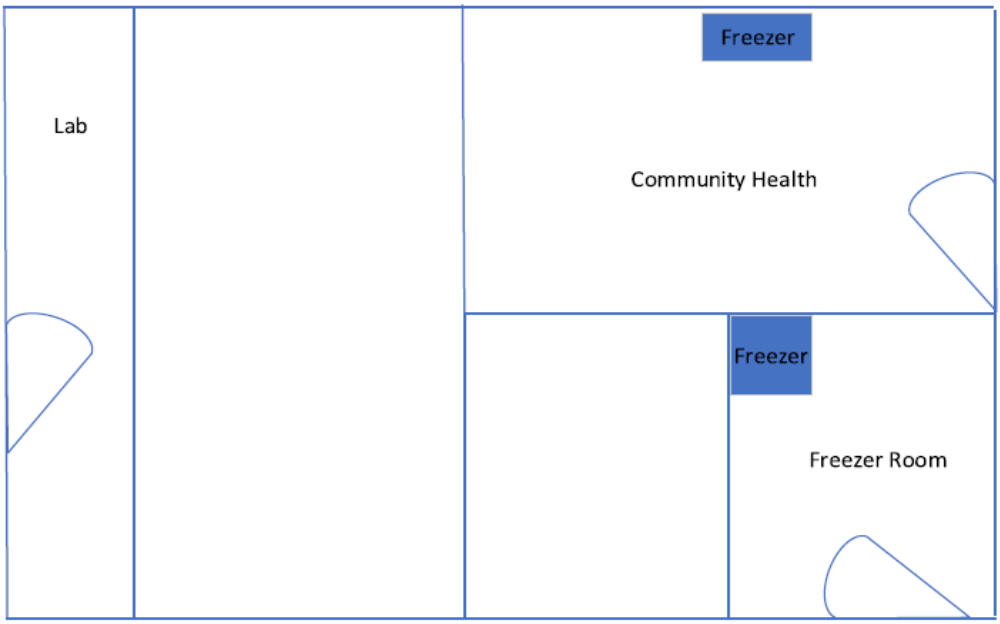
# APPENDIX 2 TO ANNEX A – ENVIRONMENTAL MONITORING SYSTEM – ACCEPTANCE TESTING CHECKLIST

**APPENDIX 2 - ENVIRONMENTAL MONITORING SYSTEM - ACCEPTANCE TESTING CHECKLIST**

| Test # | Environmental Monitoring Systems (EMS) : functions to be tested | Mean of compliance | Pass | Fail | Comments |
|---|---|---|---|---|---|
| T1 | 5.3. The software must be accessible from mobile devices or personal computers. | One of the 2 options :<br>1-Software web link<br>2-Desktop application and mobile application | | | |
| T2 | 5.5. The software must support user authentication with a personal user ID and password | Obtain Administrator (Admin) User ID and password from Contractor<br>Log in Admin account with Admin User ID and password<br>Create 4 other accounts from Admin account<br>Log in these 4 accounts with their User ID and password created | | | |
| T3 | 5.6. The software must enable the creation of different user profiles:<br>5.6.1. Administrator<br>5.6.2. Supervisor<br>5.6.3. User<br>5.6.4. Quality assurance | Software test bench fom Admin account :<br>Create supervisor profile and assign 2 accounts created in test T2 (now called accounts S1 and S2)<br>Create user profile and assign the 2 other accounts created in test T2 (now called accounts U1 and U2)<br>Create quality assurance profile | | | |
| T4 | 4.5. The environmental monitoring systems of the thirty (30) sites must be connected on the same software. | Software test bench from Admin account :<br>Create thirty (30) sites on the software (name one of them L1 and the other L2) | | | |
| T5 | 5.2. The software must enable assigning a location and identifier to each device | Software test bench from Admin account :<br>Connect 2 new probes-transmitters to the software. They must be detected by the software and visible in the list of devices.<br>Assign identifiers to the devices (now called P1 and P2)<br>Assign 2 different locations to the devices among the twenty nine (29) sites. (P1 is located at L1 and P2 is located at L2) | | | |
| T6 | 5.7. The software must enable view, edit, add, delete restrictions on each user profile on the following parameters :<br>5.7.1. Device access<br>5.7.2. User permissions | Software test bench from Admin account :<br>Admin : must be able to view edit add delete every device for every location, meaning P1 and P2<br><br>Assign L1 as a location for accounts S1 and U1<br>S1 : must be able to view edit add delete every device for their location, meaning P1<br>U1 : must be able to view only every device for their location , meaning P1<br><br>Assign L2 as a location for accounts S2 and U2<br>S2 : must be able to view edit add delete every device for their location, meaning P2<br>U2 : must be able to view only every device for their location , meaning P2 | | | |
| T7 | 5.8. The software must allow for the complete remote configuration of the devices including the following:<br>5.8.1. Sampling intervals<br>5.8.2. Temperature limits<br>5.8.3. Alarms setups<br>5.8.4. Reports configuration | Software test bench for one device (example P1) :<br>Set sampling time at five (5) minutes<br>Set temperature limits for -25-15 for a freezer and 2-8 for a refrigerator<br>Generate a report from the beginning (at least 24h) | | | |
| T8 | 5.9. The software must allow tiered alarm management including :<br>5.9.1. Unlimited number of alarms to be sent by text message, phone, e-mail.<br>5.9.2. Alarms to be sent to up to four (4) separate points of contact.<br>5.9.3. Alarms must have a configurable frequency for sending alerts which have not been responded to. | Software test bench from supervisor account (example S1) :<br>Specify U1 as the primary contact for receiving alarms<br>Specify text message and email as methods for sending the alarm<br>Specify alarm frequency to one (1) minute<br>Put the temperature outside the range and verify if the alarms are sent as specified | | | |
| T9 | 4.8. The environmental monitoring systems must include audible and visible alarms for each freezer and refrigerator. | Put the temperature outsite the range and verify if visible and audible alarms are triggered on the device | | | |
| T10 | 4.4. The environmental monitoring system must have real time data collection and real time data transfer to a secured central web-based platform (software). The delay between present temperature and reported temperature in the software must be no more than one (1) hour. | Software test bench from supervisor account (example S1):<br>Temperatures with date and time are reported in the software for P1 in less than one hour | | | |
| T11 | 5.12. The software must provide data history for each sensor. Data must be available for export into Microsoft Excel. | Software test bench from user account (example U1)<br>Verify in the software if history of temperatures is available for P1. Export the data into Microsoft Excel | | | |

## APPENDIX 3 TO ANNEX A - LAYOUT OF REFRIGERATORS AND FREEZERS PER LOCATION

Kingston - Main Clinic



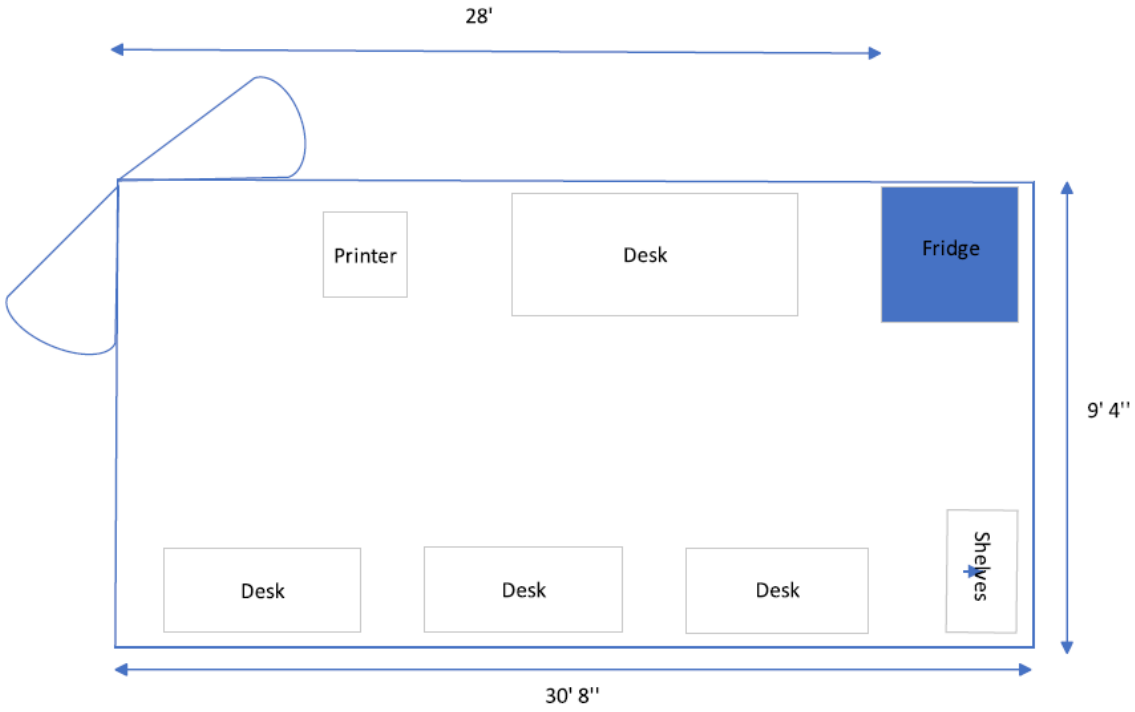
National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

Kingston - Pharmacy

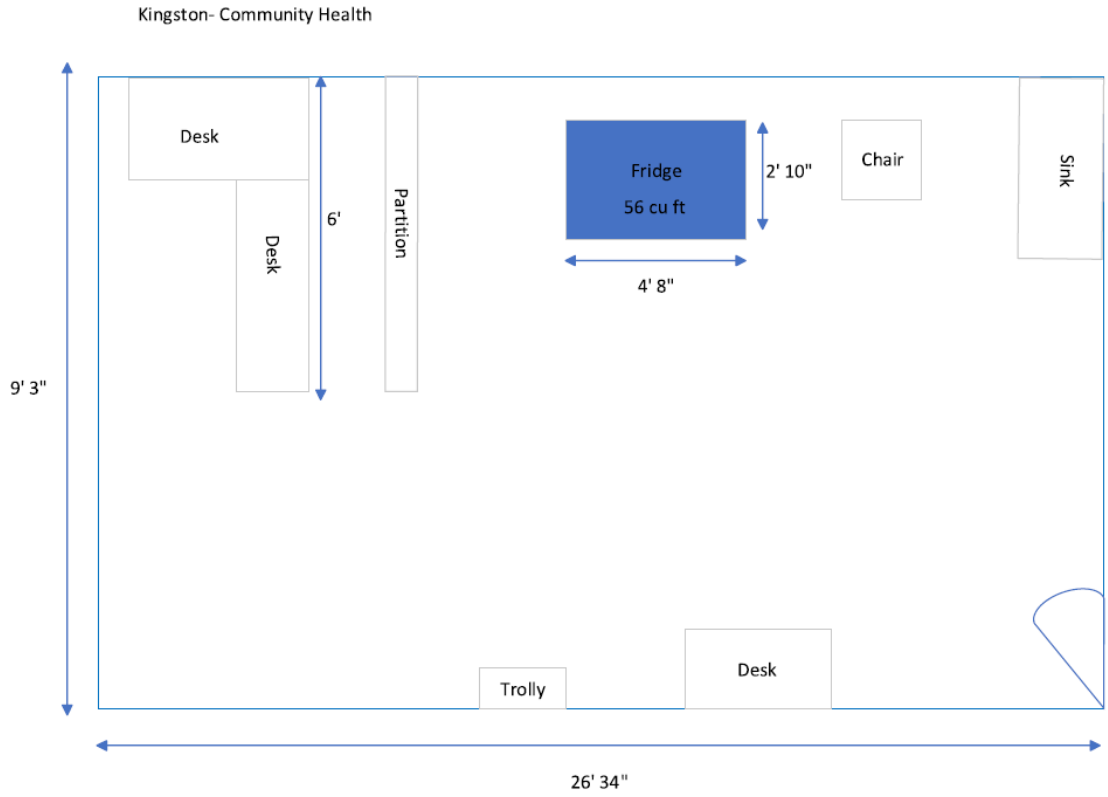


National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

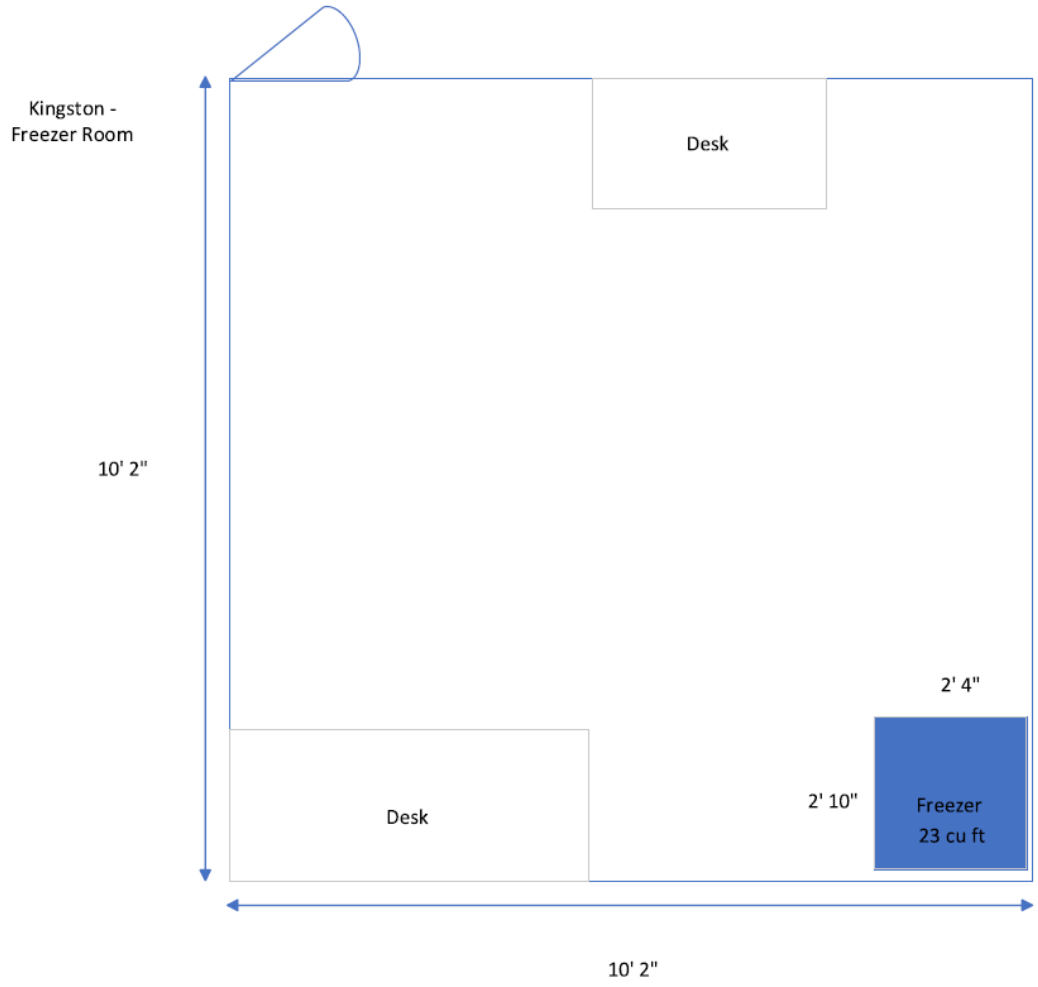


National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

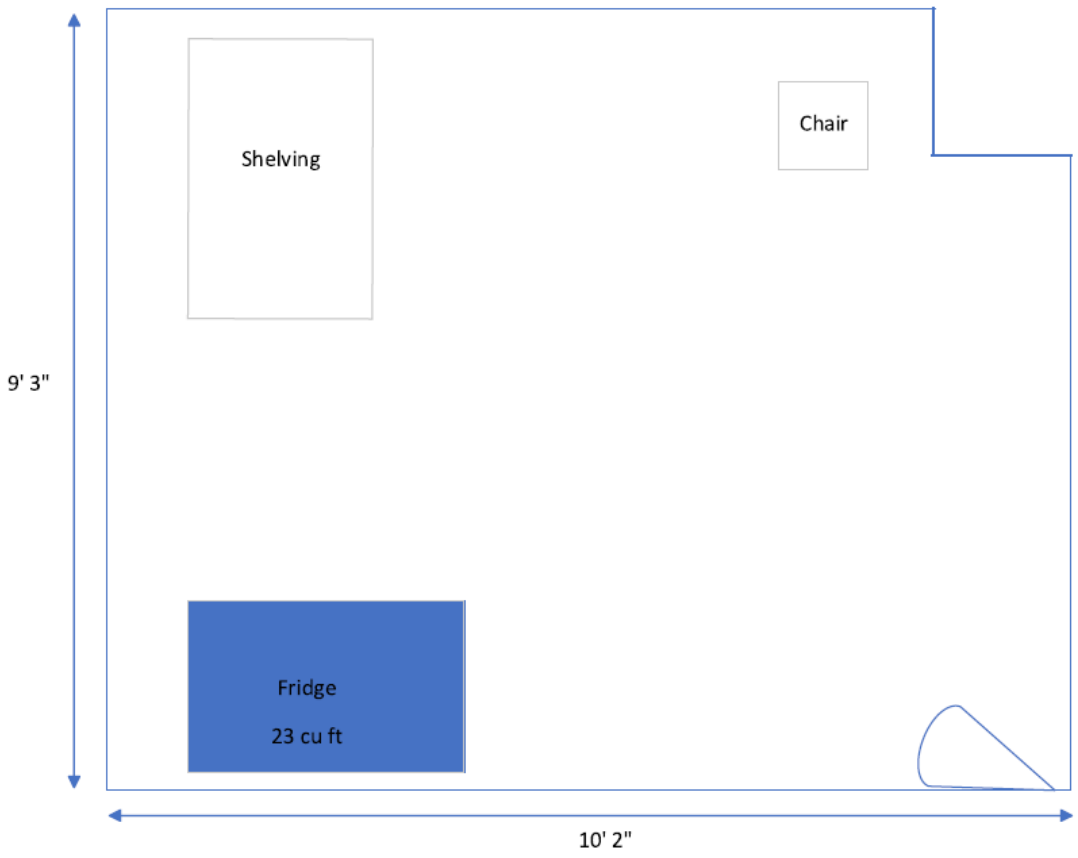
Défense nationale

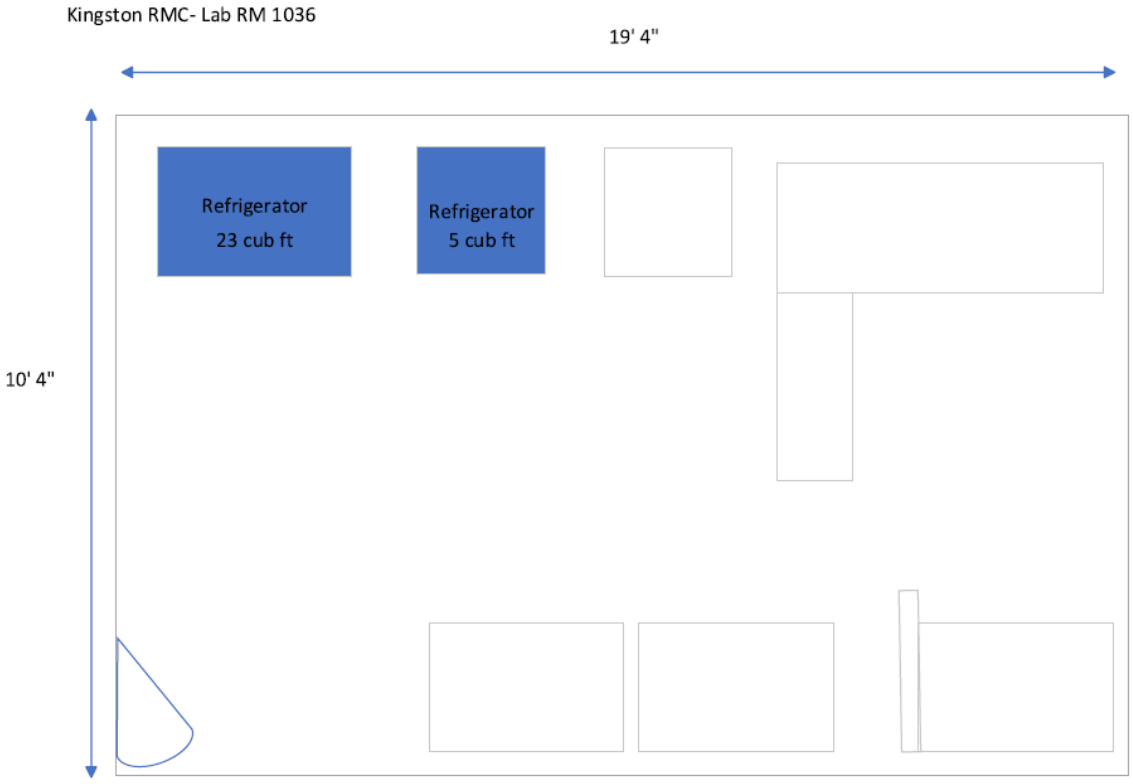
Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2




Canada

Kingston - Lab Cold Room



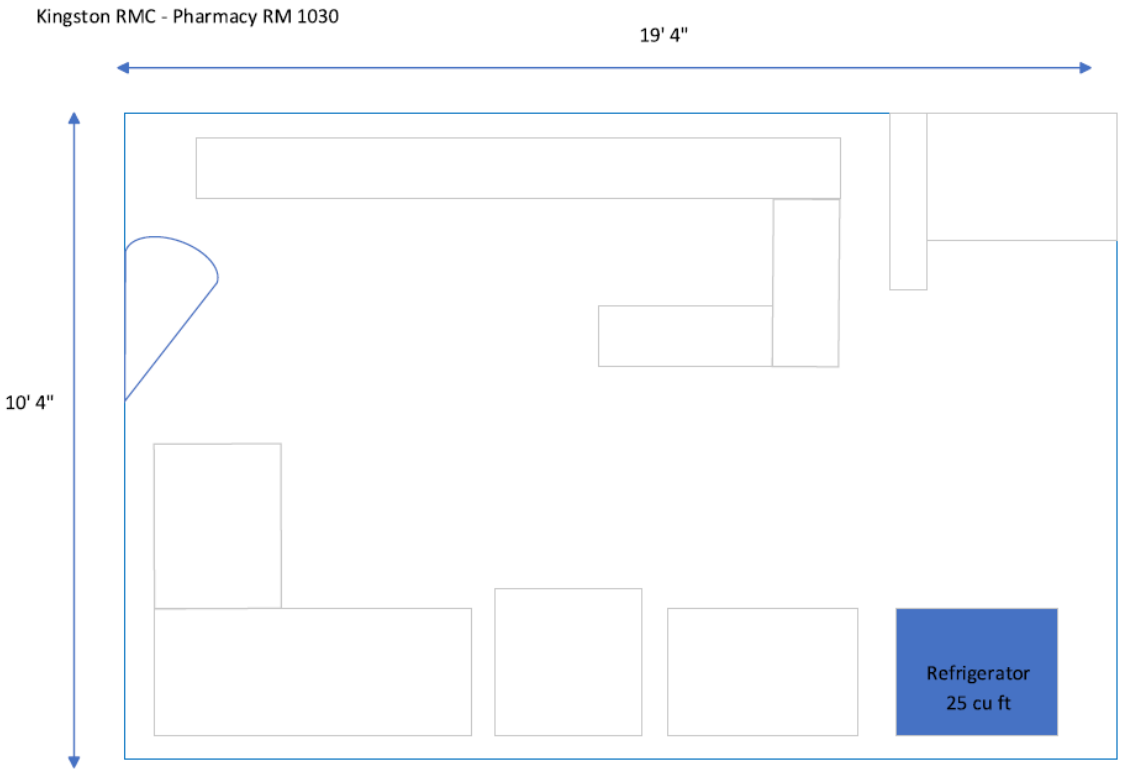

Kingston RMC- Lab RM 1036
19' 4"
10' 4"
Refrigerator
23 cub ft
Refrigerator
5 cub ft

National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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



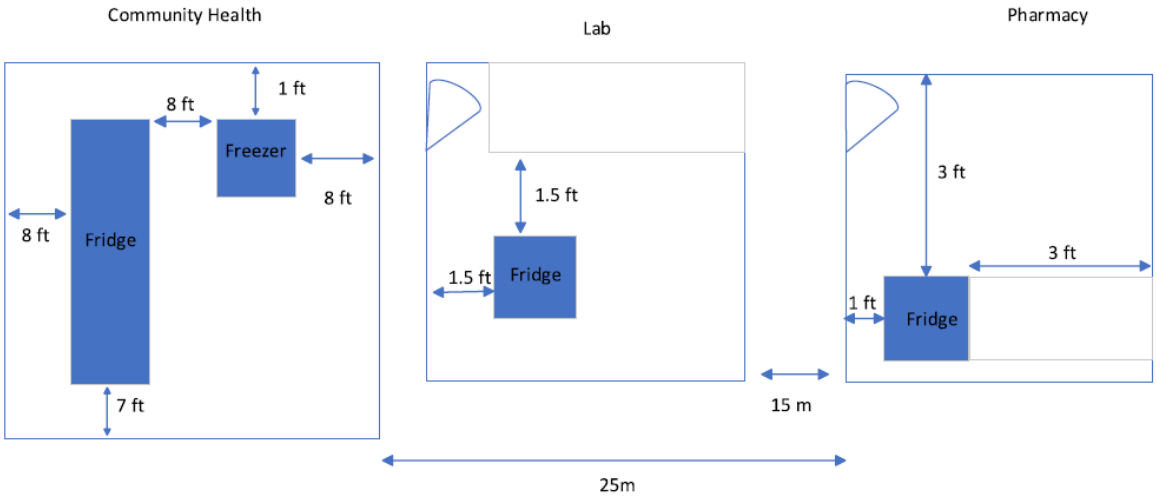
National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

Borden



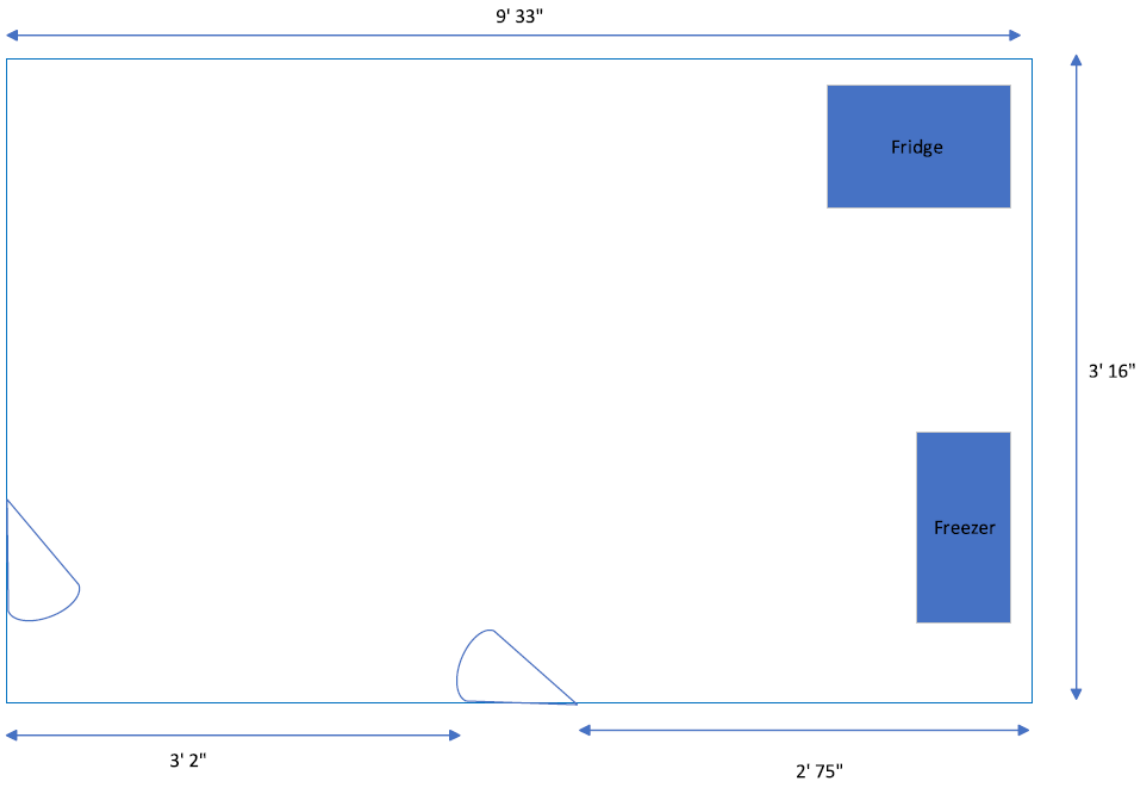
National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

Dundurn



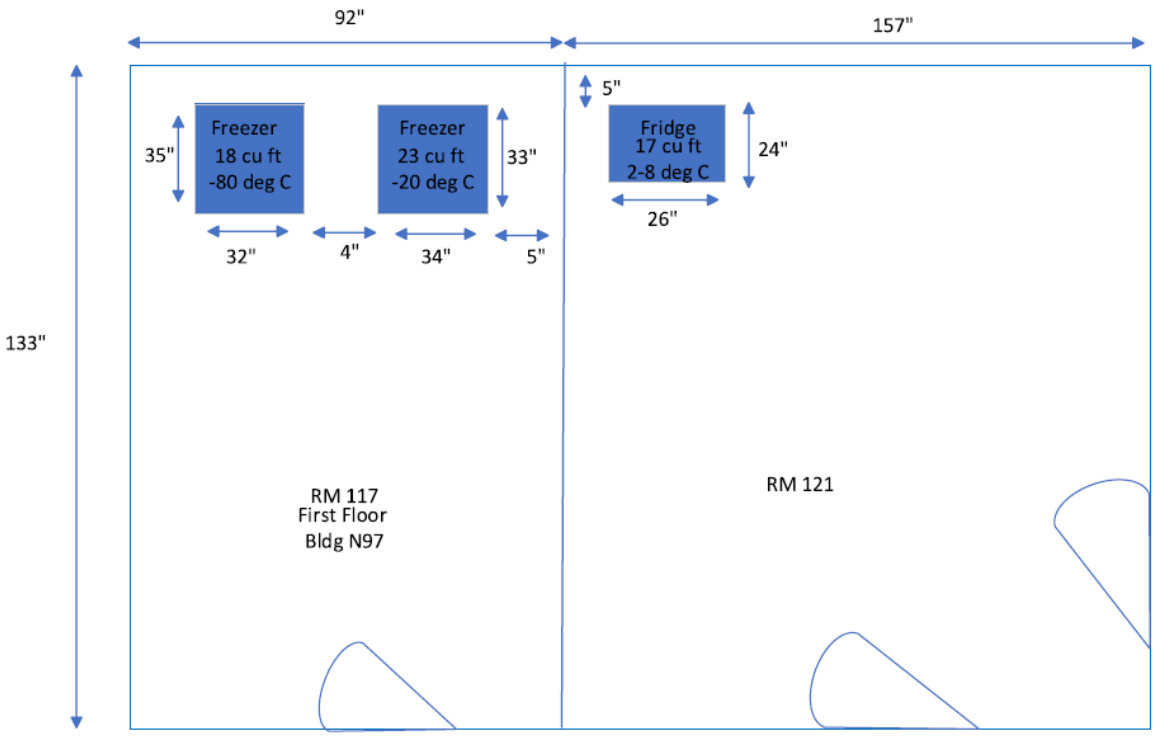
National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

Esquimalt - Room 117 & 121



National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

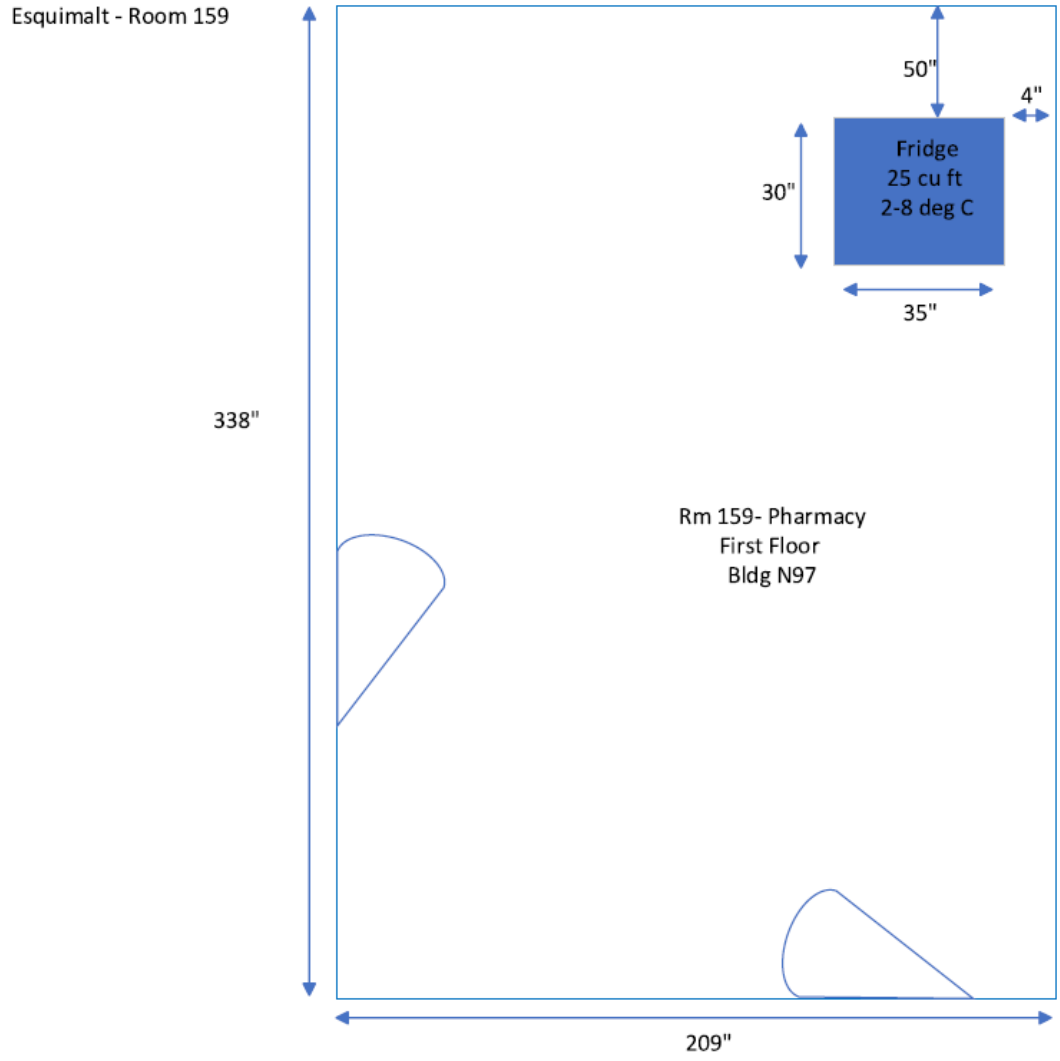
Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

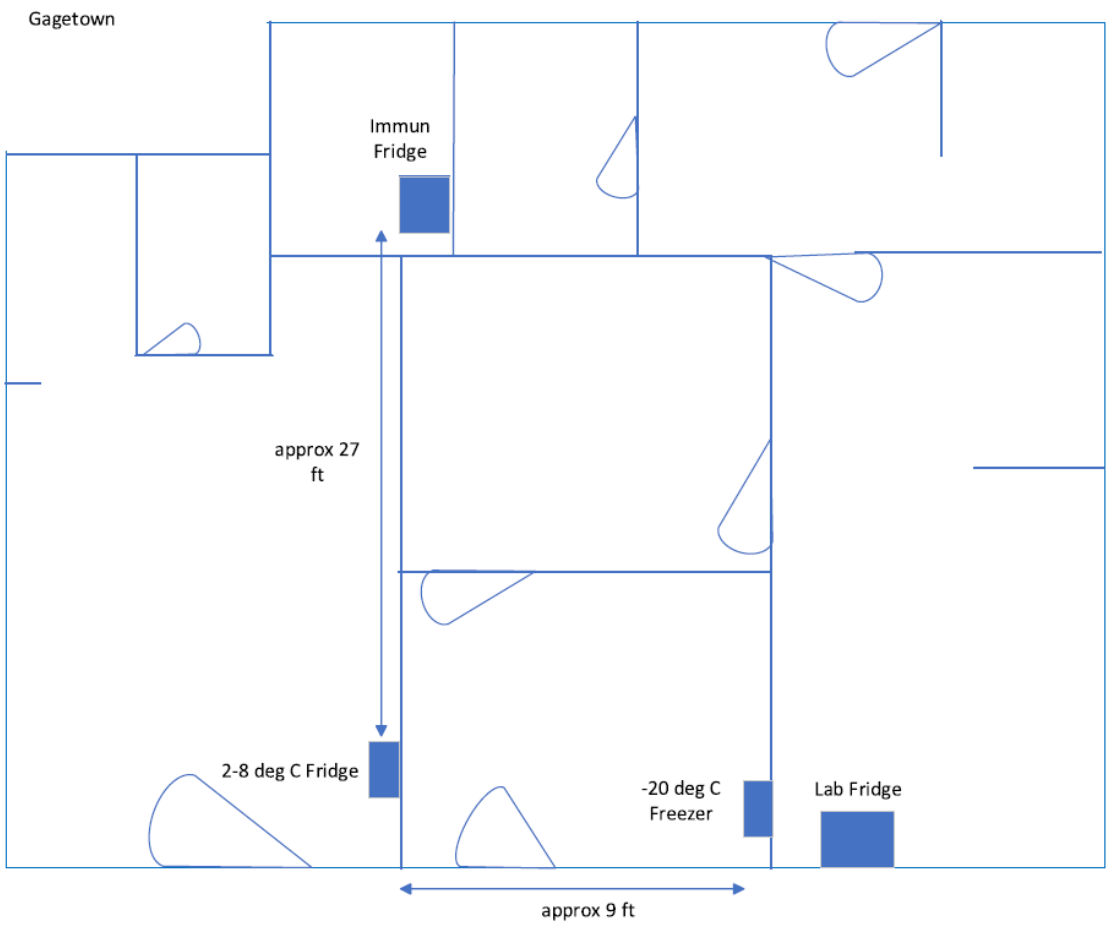


National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

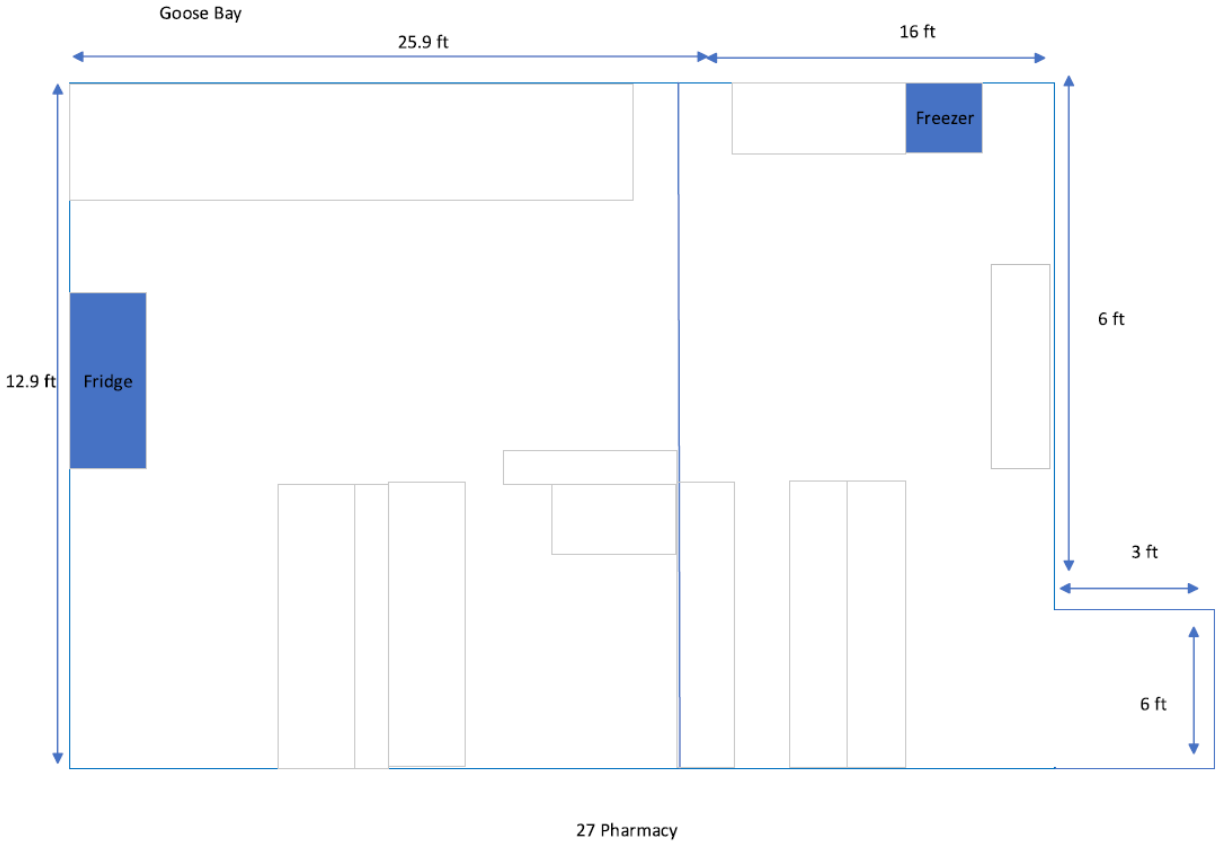


National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

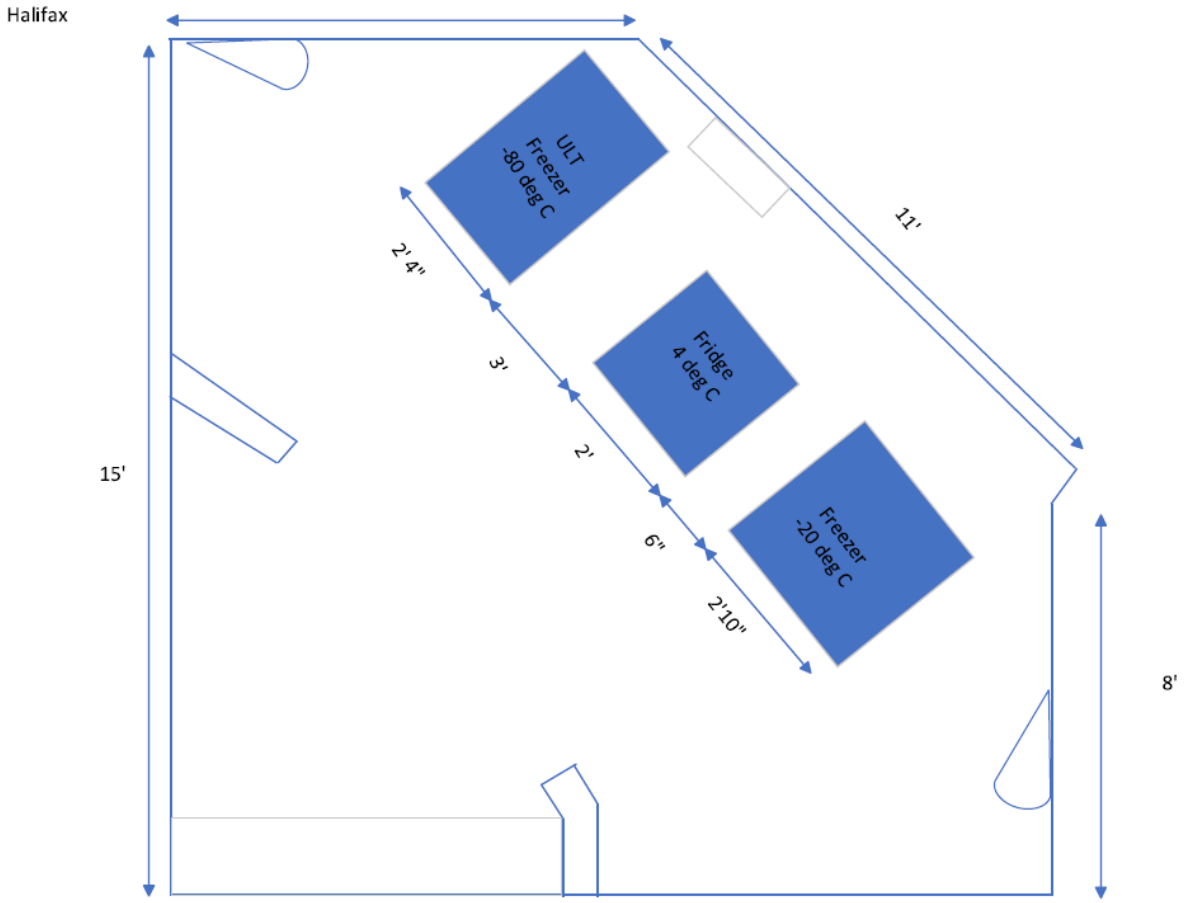


National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

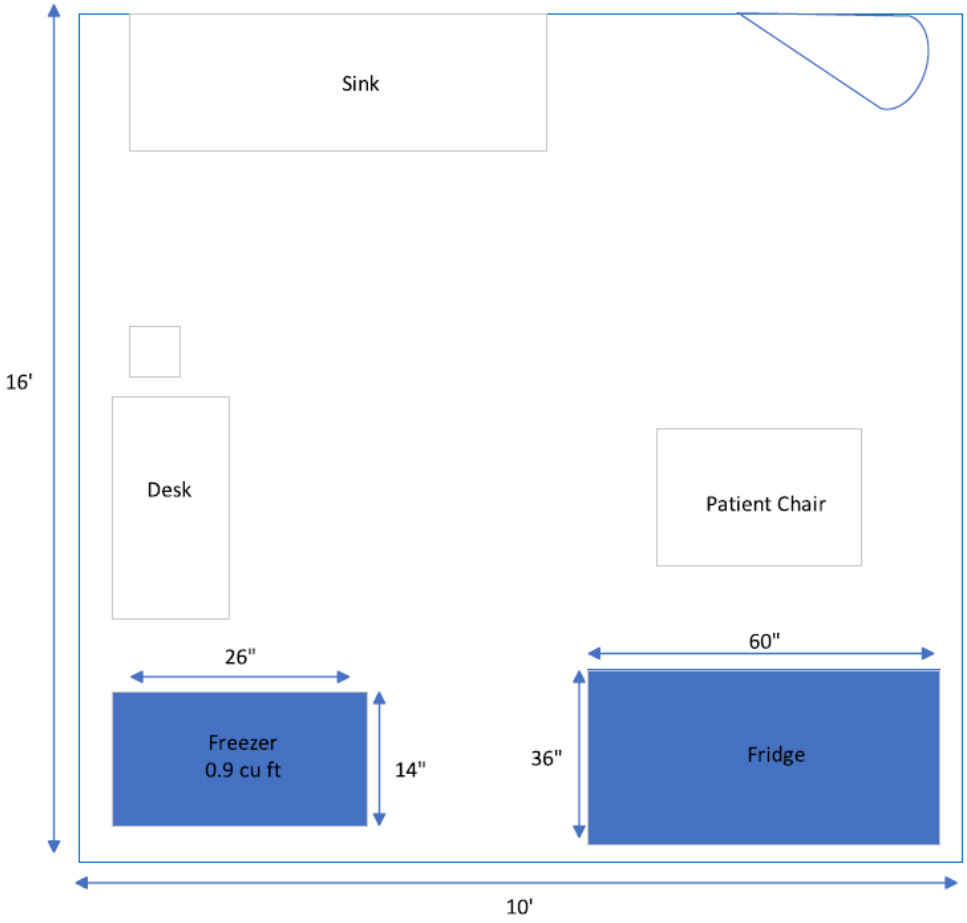
Défense nationale

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



Longue-Pointe

Immunization Room- Longue-Pointe- Montreal

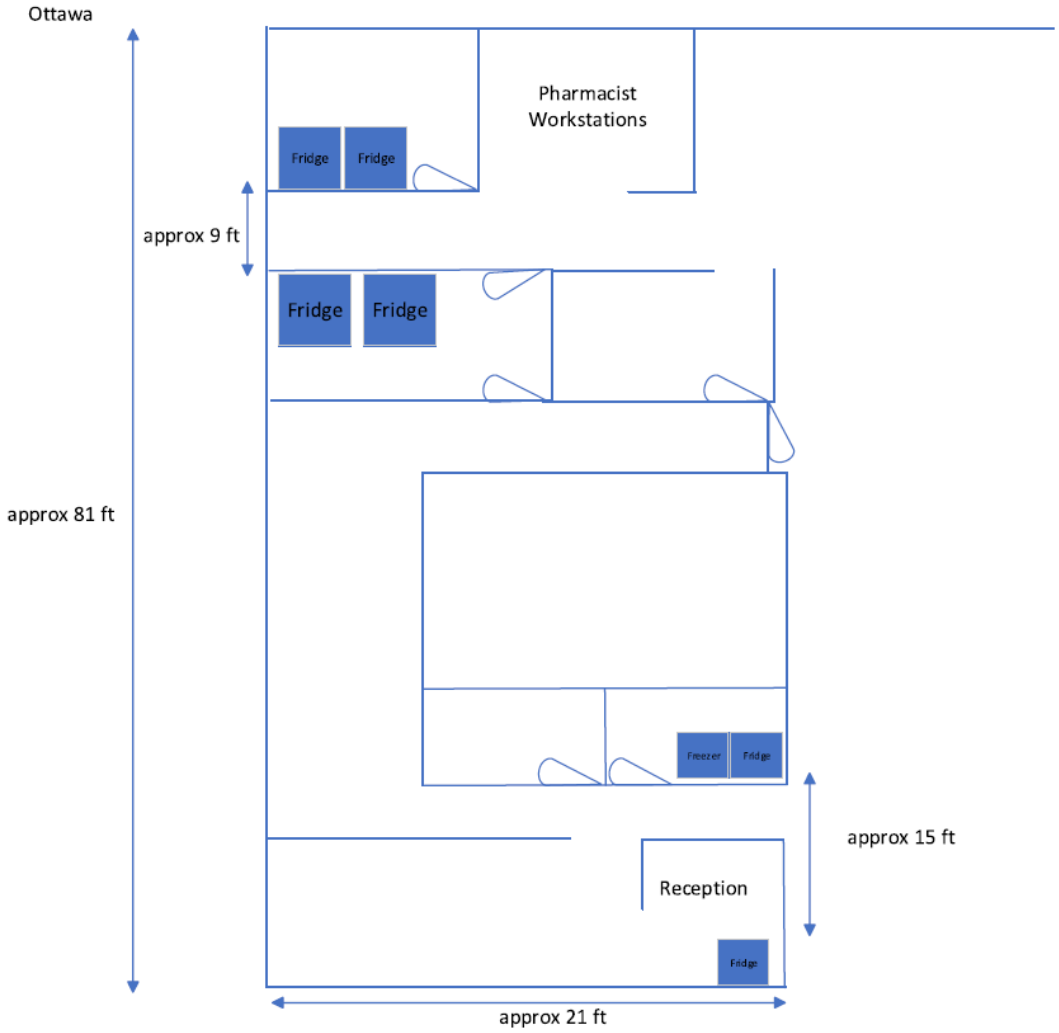


National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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



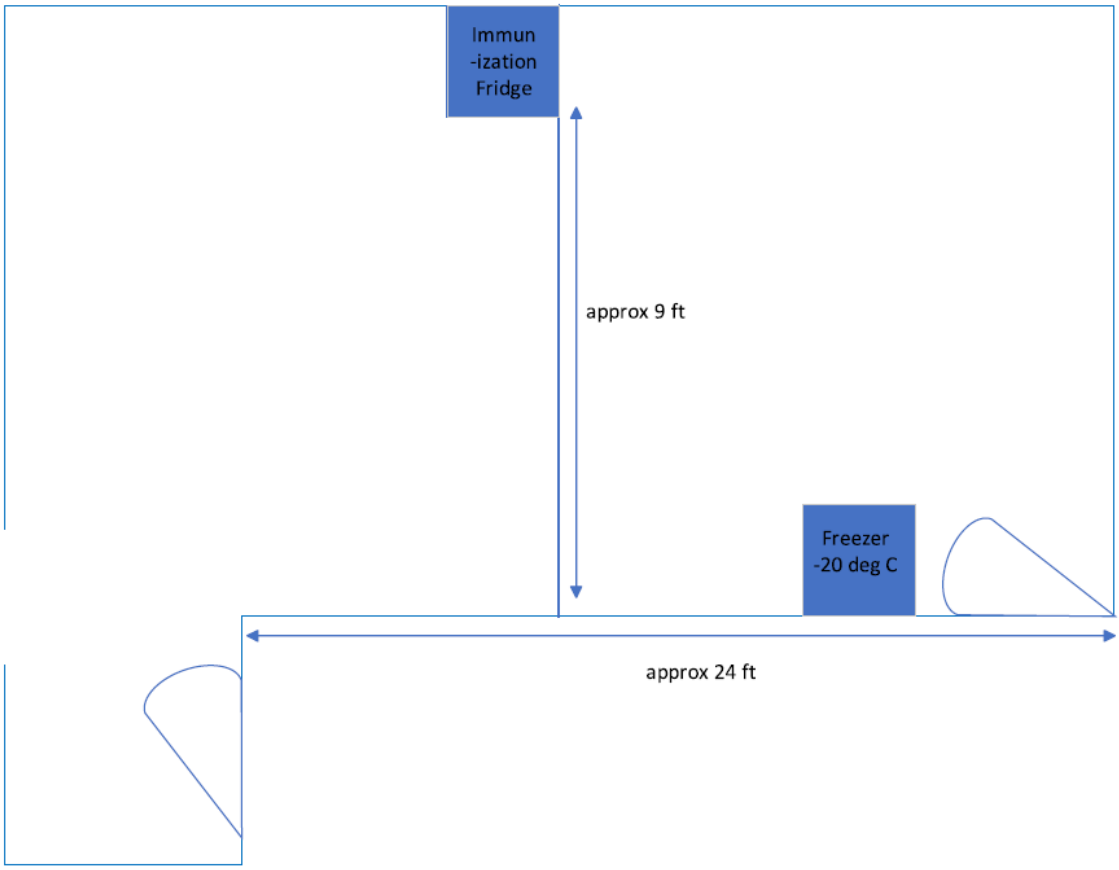
National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

St-John



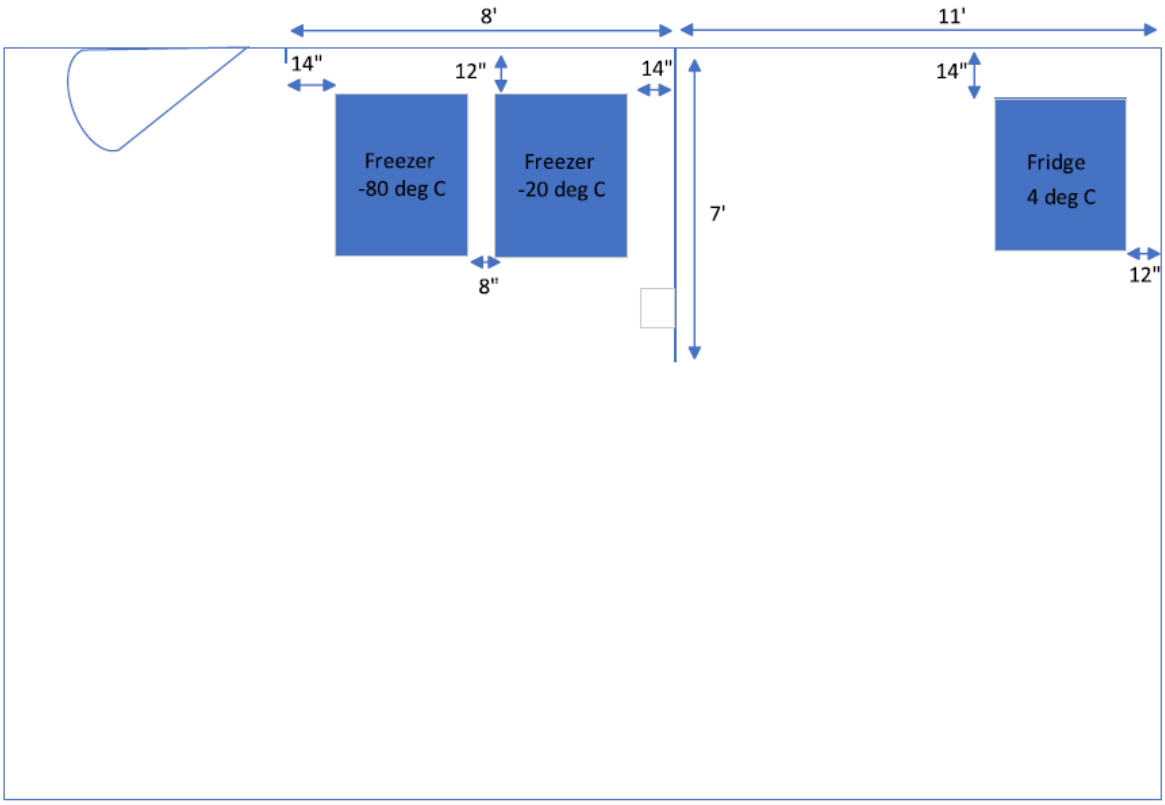
National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

Valcartier



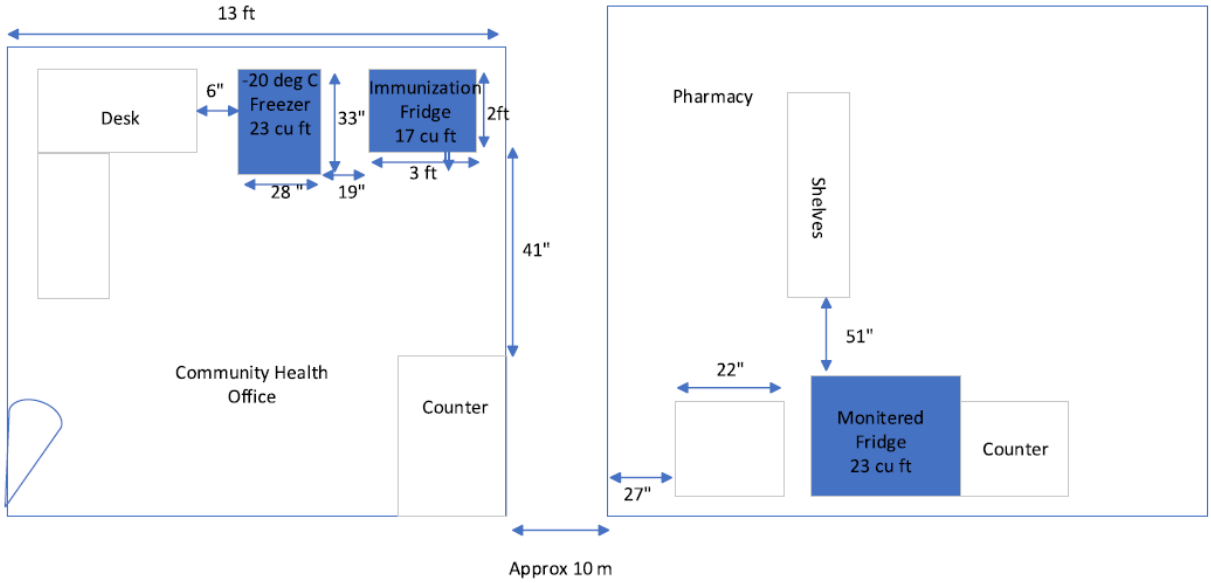
National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

Wainright



National Defence

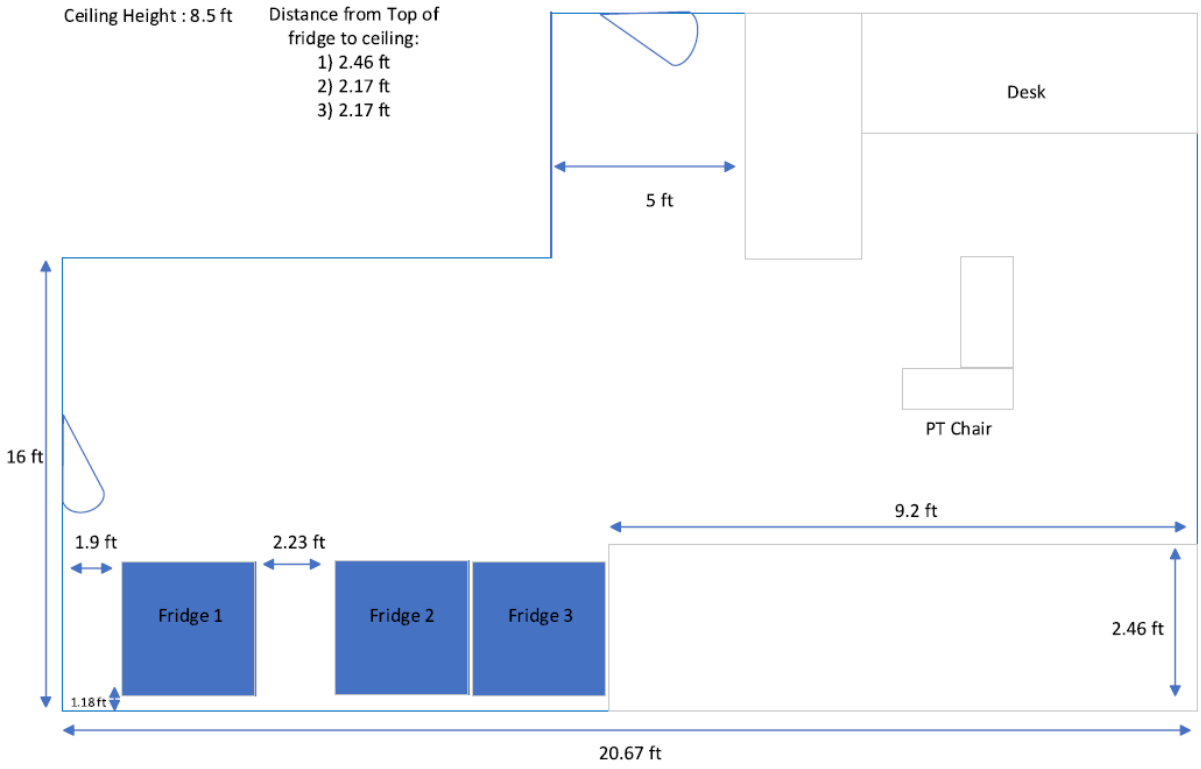
National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

Winnipeg

23 CFHSC - IMMUNZ RM 214 SCHEMATIC



## ANNEX B - BASIS OF PAYMENT

The Contractor shall be paid the firm unit prices, Delivered at Place (DAP) to the delivery location mentioned in Annex A.

The Contractor is responsible for export clearance, delivery charges, administration, costs and risks of transport. DND is responsible for all import clearance, including the payment of applicable duties and taxes. The total amount of Goods and Services Tax (GST) or Harmonized Sales Tax (HST) is to be shown separately, if applicable.

### 1.0 INITIAL CONTRACT PERIOD: FROM DATE OF CONTRACT AWARD TO 31 MARCH 2024. ALL ITEMS MUST BE DELIVERED BY 30 AUGUST 2023.

| ITEM NO. | DESCRIPTION | QTY | UNIT OF ISSUE | FIRM UNIT PRICE (CAD$) |
|---|---|---|---|---|
| **1.0** | **EQUIPMENT** | | | |
| 1.1 | -80 ºC freezer probe-transmitter and its Certificate of Calibration testing, as referenced in Annex A, para 2.1.1.1 herein | Up to 5 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.2 | -20ºC freezer probe-transmitter and its Certificate of Calibration testing, as referenced in Annex A, para 2.1.1.1 herein | Up to 30 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.3 | 2 ºC to 8 ºC refrigerator probe-transmitter and its Certificate of Calibration testing, as referenced in Annex A, para 2.1.1.1 herein | Up to 61 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.4 | Receivers-gateways fitted with Global System for Mobile communications (GSM) router, as referenced in Annex A, para 2.1.1.2 herein | 1 | Lot | **$[amount to be detailed in the resulting contract]** |
| 1.5 | Software package for all the probes-transmitters with unlimited number of users and unlimited alarms (phone, email, text), as referenced in Annex A, para 2.1.2.1 herein | 1 | Each | **$[amount to be detailed in the resulting contract]** |

| | | | | |
|---|---|---|---|---|
| 1.6 | Cellular network plan for all the receivers-gateways as referenced in Annex A, para 2.1.2.2 herein | 1 | Each | **$[amount to be detailed in the resulting contract]** |
| **2.0** | **TRAINING** | | | |
| 2.1 | Virtual Operator Training Session for 5 to 10 operators per session as described in Annex A, para 9.1 herein. | Up to 30 | Session | **$[amount to be detailed in the resulting contract]** |
| 2.2 | Technical Service Training for 2 to 8 Biomedical Engineering Technologists per session as described in Annex A, para 9.2 herein. | 1 | Session | **$[amount to be detailed in the resulting contract]** |

**2.0 OPTIONAL REQUIREMENT: FROM 01 APRIL 2024 TO 31 MARCH 2027. ALL ITEMS MUST BE DELIVERED BY 31 MARCH 2027.**

**2.1 OPTIONAL REQUIREMENT – YEAR 1: 01 APRIL 2024 TO 31 MARCH 2025**

| ITEM NO. | DESCRIPTION | QTY | UNIT OF ISSUE | FIRM UNIT PRICE (CAD$) |
|---|---|---|---|---|
| **1.0** | **EQUIPMENT** | | | |
| 1.1 | Any type of probe-transmitter among -80 °C, -20°C, 2 °C to 8 °C, with its Certificate of Calibration testing, as referenced in Annex A, para 2.2.1.1 herein | Up to 24 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.2 | Receiver-gateway fitted with Global System for Mobile communications (GSM) router, as referenced in Annex A, para 2.2.1.2 herein | Up to 6 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.3 | Software package for one (1) additional probe-transmitter for one (1) year, as referenced in Annex A, para 2.2.3.1 herein | Up to 24 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.4 | Cellular plan for one (1) additional receiver-gateway for one (1) year, as referenced in Annex A, para 2.2.3.3 herein | Up to 6 | Each | **$[amount to be detailed in the resulting contract]** |

| | | | | |
|---|---|---|---|---|
| 1.5 | Software package for initial probes-transmitters as referenced in Annex A, para 2.2.3.2 herein | 1 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.6 | Cellular network plan for initial receivers-gateways as referenced in Annex A, para 2.2.3.4 herein | 1 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.7 | Offsite calibration of probes, as referenced Annex A, para 2.2.2.3 herein | 1 | Service | **$[amount to be detailed in the resulting contract]** |
| **2.0** | **TRAINING** | | | |
| 2.1 | Virtual Operator Training Session for 5 to 10 operators per session as described in Annex A, para 9.1 herein | Up to 10 | Session | **$[amount to be detailed in the resulting contract]** |
| 2.2 | Technical Service Training for 2 to 8 Biomedical Engineering Technologists per session as described in Annex A, para 9.2 herein | 1 | Session | **$[amount to be detailed in the resulting contract]** |

**2.2 OPTIONAL REQUIREMENT – YEAR 2: 01 APRIL 2025 TO 31 MARCH 2026**

| ITEM NO. | DESCRIPTION | QTY | UNIT OF ISSUE | FIRM UNIT PRICE (CAD$) |
|---|---|---|---|---|
| **1.0** | **EQUIPMENT** | | | |
| 1.1 | Any type of probe-transmitter among -80 °C, -20°C, 2 °C to 8 °C, with its Certificate of Calibration testing, as referenced in Annex A, para 2.2.1.1 herein | Up to 24 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.2 | Receiver-gateway fitted with Global System for Mobile communications (GSM) router, as referenced in Annex A, para 2.2.1.2 herein | Up to 6 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.3 | Software package for one (1) additional probe-transmitter for one (1) year, as referenced in Annex A, para 2.2.3.1 herein | Up to 48 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.4 | Cellular plan for one (1) additional receiver-gateway for one (1) year, as referenced in Annex A, para 2.2.3.3 herein | Up to 12 | Each | **$[amount to be detailed in the resulting contract]** |

| | | | | |
|---|---|---|---|---|
| 1.5 | Software package for initial probes-transmitters as referenced in Annex A, para 2.2.3.2 herein | 1 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.6 | Cellular network plan for initial receivers-gateways as referenced in Annex A, para 2.2.3.4 herein | 1 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.7 | Offsite calibration of probes, as referenced Annex A, para 2.2.2.3 herein | 1 | Service | **$[amount to be detailed in the resulting contract]** |
| **2.0** | **TRAINING** | | | |
| 2.1 | Virtual Operator Training Session for 5 to 10 operators per session as described in Annex A, para 9.1 herein. | Up to 10 | Session | **$[amount to be detailed in the resulting contract]** |
| 2.2 | Technical Service Training for 2 to 8 Biomedical Engineering Technologists per session as described in Annex A, para 9.2 herein. | 1 | Session | **$[amount to be detailed in the resulting contract]** |

**2.3 OPTIONAL REQUIREMENT – YEAR 3: 01 APRIL 2026 TO 31 MARCH 2027**

| ITEM NO. | DESCRIPTION | QTY | UNIT OF ISSUE | FIRM UNIT PRICE (CAD$) |
|---|---|---|---|---|
| **1.0** | **EQUIPMENT** | | | |
| 1.1 | Any type of probe-transmitter among -80 °C, -20°C, 2 °C to 8 °C, with its Certificate of Calibration testing, as referenced in Annex A, para 2.2.1.1 herein | Up to 24 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.2 | Receiver-gateway fitted with Global System for Mobile communications (GSM) router, as referenced in Annex A, para 2.2.1.2 herein | Up to 6 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.3 | Software package for one (1) additional probe-transmitter for one (1) year, as referenced in Annex A, para 2.2.3.1 herein | Up to 72 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.4 | Cellular plan for one (1) additional receiver-gateway for one (1) year, as referenced in Annex A, para 2.2.3.3 herein | Up to 18 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.5 | Software package for initial probes-transmitters as referenced in Annex A, para 2.2.3.2 herein | 1 | Each | **$[amount to be detailed in the resulting contract]** |

| | | | | |
|---|---|---|---|---|
| 1.6 | Cellular network plan for initial receivers-gateways as referenced in Annex A, para 2.2.3.4 herein | 1 | Each | **$[amount to be detailed in the resulting contract]** |
| 1.7 | Offsite calibration of probes, as referenced Annex A, para 2.2.2.3 herein | 1 | Service | **$[amount to be detailed in the resulting contract]** |
| **2.0** | **TRAINING** | | | |
| 2.1 | Virtual Operator Training Session for 5 to 10 operators per session as described in Annex A, para 9.1 herein. | Up to 10 | Session | **$[amount to be detailed in the resulting contract]** |
| 2.2 | Technical Service Training for 2 to 8 Biomedical Engineering Technologists per session as described in Annex A, para 9.2 herein. | 1 | Session | **$[amount to be detailed in the resulting contract]** |

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

# ANNEX C - SECURITY REQUIREMENTS CHECK LIST

Government of Canada / Gouvernement du Canada

| Contract Number / Numéro du contrat |
|---|
| W6369-22-A009 Amendment 1 |
| Security Classification / Classification de sécurité<br>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<br>**Department of National Defence** | 2. Branch or Directorate / Direction générale ou Direction<br>DHSD/J4 Med Equip |
| 3. a) Subcontract Number / Numéro du contrat de sous-traitance | 3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant |

4. Brief Description of Work / Brève description du travail

The Department of National Defence (DND) has a requirement for the supply of environmental monitoring systems fitted with data loggers and alarms to continuously and remotely monitor the temperature of 2 oC to 8 oC refrigerators as well as -20oC and -80oC freezers deployed for the storage of COVID-19 vaccines.

| | | |
|---|---|---|
| 5. a) Will the supplier require access to Controlled Goods?<br>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?<br>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?<br>Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?<br>(Specify the level of access using the chart in Question 7. c)<br>(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.<br>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?<br>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<br>Aucune restriction relative à la diffusion ☑ | All NATO countries<br>Tous les pays de l'OTAN ☐ | No release restrictions<br>Aucune restriction relative à la diffusion ☐ |
| Not releasable<br>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) ☐ |

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

Government of Canada | Gouvernement du Canada

| Contract Number / Numéro du contrat |
|---|
| W6369-22-A009 Amendment 1 |
| 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 : Secret required only for those identified in the Cloud IT Security Obligations document, serial 29 para c.

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?

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

Government of Canada | Gouvernement du Canada

| Contract Number / Numéro du contrat |
|---|
| W6369-22-A009 Amendment 1 |
| 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 / TRES SECRET |
| Information / Assets / Renseignements / Biens | ✓ | | | | | | | | | | | | | | | |
| Production | | | | | | | | | | | | | | | | |
| IT Media / Support TI | ✓ | | | | | | | | | | | | | | | |
| IT Link / Lien électronique | | | | | | | | | | | | | | | | |

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

[Page 4 of the SRCL to be inserted in the resulting contract]

## APPENDIX 1 TO ANNEX C – SRCL SUPPLEMENTAL SECURITY GUIDE

### Part A - Multiple Release Restrictions: Security Guide

**To be completed in addition to SRCL question 7.b) when release restrictions are therein identified. Indicate to which levels of information release restrictions apply. Make note in the chart if a level of information bears multiple restrictions (e.g. a portion of the SECRET information bears the caveat Canadian Eyes Only while the remainder of the SECRET information has no release restrictions.)**

**Canadian Information**

| Citizenship Restriction | PROTECTED | | | CLASSIFIED | | | |
|---|---|---|---|---|---|---|---|
| | A | B | C | CONFIDENTIAL | SECRET | TOP SECRET | TOP SECRET (SIGINT) |
| No Release Restrictions | X | | | | | | |
| Not Releasable | | | | | | | |
| Restricted to: | | | | | | | |
| Permanent Residents Included* | | | | | | | |

**NATO Information**

| Citizenship Restriction | NATO UNCLASSIFIED | NATO RESTRICTED | NATO CONFIDENTIAL | NATO SECRET | COSMIC TOP SECRET |
|---|---|---|---|---|---|
| All NATO Countries | | | | | |
| Restricted to: | | | | | |
| Permanent Residents Included* | | | | | |

**Foreign Information**

| Citizenship Restriction | PROTECTED | | | CLASSIFIED | | | |
|---|---|---|---|---|---|---|---|
| | A | B | C | CONFIDENTIAL | SECRET | TOP SECRET | TOP SECRET (SIGINT) |
| No Release Restrictions | | | | | | | |
| Restricted to : | | | | | | | |
| Permanent Residents Included* | | | | | | | |

**COMSEC Information**

| Citizenship Restriction | PROTECTED | | | CLASSIFIED | | | |
|---|---|---|---|---|---|---|---|
| | A | B | C | CONFIDENTIAL | SECRET | TOP SECRET | TOP SECRET (SIGINT) |
| Not Releasable | | | | | | | |
| Restricted to: | | | | | | | |

***When release restrictions are indicated, specify if permanent residents are allowed to be included.**

| Part B - Multiple Levels of Personnel Screening: Security Classification Guide<br>**To be completed in addition to SRCL question 10.a) when multiple levels of personnel screening are therein identified. Indicate which personnel screening levels are required for which portions of the work/access involved in the contract.** | | | |
|---|---|---|---|
| Level of Personnel Clearance (e.g. Reliability, Secret) | Position / Description/Task | Access to sites and/or information. Levels of Information to be accessed. | Citizenship Restriction (if any) |
| Reliability | Contractor Personnel with access to DND's data | 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. | |
| Secret | Cloud System Administrator or Privileged Users | The contract's cloud IS must be administered and maintained by individual(s) possessing - at minimum - a valid Secret (Level II) Security Clearance. | |
| | | | |
| | | | |
| | | | |
| | | | |

| Part C – Safeguards / Information Technology (IT) Media – 11d = yes |
|---|
| IT security requirements must be specified in a separate technical document and submitted with the SRCL |

**OTHER SECURITY INSTRUCTIONS**

Contractor personnel require reliability status unless otherwise specified within the "Cloud IT Security Obligations" document

National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

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

**APPENDIX 2 TO ANNEX C – INFORMATION TECHNOLOGY SECURITY REQUIREMENTS**

# Department of National Defence (DND)

# Information Technology Security Requirements Document

# for

# Contract W6369-22-A009 Amendment 1

## 1. Introduction

**1.1** The IT Security Requirements Document. This "IT Security Requirements Document for Contract W6369-22-A009 Amendment 1 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 for which it is written. Accordingly this "IT Security Requirements Document for Contract W6369-22-A009 Amendment 1 is specific to Contract W6369-22-A009 Amendment 1.

**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 A.

**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 Public Services and Procurement Canada 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 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). As 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 A 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 that 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 IS - 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 not authorized for this contract.

### 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;

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; and

2.3.1.3 be a Canadian citizen.

2.3.2 Access to the Physical Security Zone. No visitors, foreign nationals or unauthorized personnel shall have access to the Proprietary Information, the IS, 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 PSPC "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 IS . 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 IS. These documents 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 during the life of this contract.

2.4.2 User Agreement Form. All personnel having access to the IS must read the system-specific IT Security Orders for the IS 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 and **Secret (Level II) Security Clearance** for Cloud's contract IS privileged users and system administrators.

2.4.4 Vulnerability Management and Incident Reporting. Per Annex A, Section VI of the CSM, a vulnerability management process must be identified and followed to ensure risks from vulnerabilities are managed. The contractor must also report any security incident to the DND Project Lead by no later than 24 hours after it has been detected or reported to PSPC.

2.4.5 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.) and all removable IT media used to store / process / create Proprietary Information must be physically locked in Government of Canada (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 should be encrypted using GC-approved encryption technology appropriate for the sensitivity level of the Proprietary Information it contains. This is to protect the information in case the IT media is lost, misplaced or stolen.

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) used to store the information.

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 IT media must be handled and transported/transmitted in accordance with GC guidelines as stated 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-approved encryption technology 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. Any IT link must first be validated, inspected, and authorized by PSPC/CSP as well as recognized and authorized by the DND IT Security Authority and the DND PO.

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 CSE publication "*IT Media Sanitization (ITSP.40.006)*".

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

2.5.7 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.

2.5.8 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 any contractor 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 a network of COTS of Probes-transmitters with short range wireless capability, Receivers-gateways fitted with Global System for Mobile communications (GSM) router provided by the contractor, CAF user will have their personal device (Laptops, tablets, Mobile Phone)

3.2.2 Type of System. The IS can be configured as Segment of a network: part of a contractor's network infrastructure which has been authorized to store / process / create the Proprietary Information. Additional security safeguards will be required to segregate the Proprietary Information from the contractor's other information. As well as GSM capability.

3.2.3 Network Security. If the IS is configured as a network, the contractor must implement perimeter defence and network security safeguards (e.g. firewalls, etc.) for the IS to negotiate all traffic and to protect servers and IT equipment that is externally accessible.

3.2.4 Segregation of IS. If configured as a segment of one of the contractor's existing networks, the contractor must segregate the networks 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.

3.2.5 Type of Equipment. The equipment used to store / process / create the Proprietary Information can consist of Commercial Off The Shelf (COTS).

3.2.6 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.

3.2.7 Operating System(s). All applicable IT equipment used for the IS must operate on supported Operating Systems (OS); i.e. the vendor of each 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 hardened; i.e. unnecessary processes, services, ports, etc. must be disabled. The IS SOP must provide details on the OS configuration and must identify the frequency and the method used to update the OS security patches.

3.2.8 Anti-virus/Anti-malware Software. A supported anti-virus/anti-malware application must be installed and operating on all applicable IT equipment. Anti-virus/anti-malware definition files

must be updated regularly - at least twice weekly, or (preferably) daily. The IS SOP must identify the frequency and the method used to update the anti-virus/anti-malware definition files as well as the configuration of the anti-virus application. Configuration of the anti-virus/anti-malware application must:

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

3.2.8.2 automatically scan all applicable IS IT equipment at power-on or on a set interval, at least weekly; and

3.2.8.3 scan every new file introduced to the IS for malicious code.

3.2.9 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. The following are the minimum IT Security Requirements/Recommendations for the web-based platform (software) solution used to monitor the refrigerators and freezers:

3.2.9.1 Web-based platform must use Secure Hypertext Transfer Protocol (HTTPS) for secure communication (encrypted) with the most recent Transport Layer Security (TLS) protocol such as; TLS 1.2 or 1.3. For securing web services, follow guidelines set forth in NIST SP 800-95 and guidelines for web services encryption, follow the guidelines set forth in NIST SP 800-175A, SP 800-175B Rev.1, FIPS 140-2 and FIPS 186-4.

3.2.9.2 Schedule website security audits to identify and address vulnerabilities, we recommend that the web application has security measures implemented to prevent the most top10 (OWASP) critical security concerns such as; Injection, Broken authentication, Sensitive data exposure, XML external entities (XXE), Broken access control, Security misconfigurations, Cross site scripting (XSS),Insecure deserialization, Using components with known vulnerabilities; and Insufficient logging and monitoring;

3.2.9.3 Update your website or software regularly;

3.2.9.4 Install security plugins and make sure they are updated;

3.2.9.5 Use automatic back-up for your website;

3.2.9.6 Establish a password authentication or a public/private key for authentication;

3.2.9.7 Enforce strong passwords and change them regularly;

3.2.9.8 Deploy two-factor authentication to access the website;

3.2.9.9 Create levels of access, limit access to the specific parts of the website they need to use to complete their day to day tasks, least privilege;

3.2.9.10 Deploy a Web application firewall (WAF);

3.2.9.11 Choose a web hosting provider that offers 24/7/365 network monitoring and firewall protection to block any known threats

3.2.9.12 Use best practices for Secure Software Development Framework (SSDF) to mitigate the risk of Software Vulnerabilities according to NIST's white paper publication https://doi.org/10.6028/NIST.CSWP.04232020 (CSWP.04232020); and

3.2.9.13 Appropriate certifications and/or accreditations for compliance must be obtained if the web applications and APIs will be processing sensitive data such as financial (PCI DSS), healthcare (HIPAA), and PII (Personally Identifiable Information) to make sure they are protected (encrypted) when in use, in transit and as well as at rest.

3.2.10 Logging and Auditing. OS logging must be active and the system administrator(s) for the IS must ensure that the logs are reviewed at least quarterly or whenever there has been a suspected compromise. The logging and 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 IS IT equipment.

3.3.3 Bluetooth Technology. The use of Bluetooth technology as part of the system's IT equipment is strictly prohibited. The use of Bluetooth technology in the Operations zone or the temporary Operations zone where the IS is located is strictly prohibited except in the case of approved medical devices; the CSO must be advised of any Bluetooth medical device that is used in the proximity of the IS and must authorize the use of this device in writing.

3.3.4 Wi-Fi or Wireless. The use of Wi-Fi or wireless capabilities as part of the IS is authorized under the following conditions:

3.3.4.1 Wi-Fi/wireless capabilities can be used at the Contractor's site(s) under the following conditions:

3.3.4.1.1 Any Wi-Fi/wireless connection to the IS must be protected by encryption. The use of WPA2 protocol is suggested; minimum encryption of 128-bit is mandatory, 256-bit encryption is highly encouraged.

3.3.4.1.2 The contractor must establish usage restrictions including access enforcement mechanisms; only authorized personnel will be given accounts on the Wi-Fi/wireless connection.

3.3.4.1.3 Best practices as outlined in CCCS publication "Annex 2 - Wireless User to Wired Network Connection High-Level Design Guidance (ITSG-41)" must be followed.

3.3.4.1.4 Modification of Wi-Fi/wireless settings is not authorized at the user level; any modifications are to be done only by the system administrator(s) and only after written agreement from the DND PO.

3.3.4.2 Wi-Fi/wireless requirements for contractor employees working remotely (i.e. MC TW employees) are covered in Section 2 above under the "Mobile Computing/ Teleworking" subsection.

3.3.4.3 Any Wi-Fi/wireless capabilities used to store / process / create Proprietary Information for this contract must first be inspected, and authorized by PSPC/CSP.

3.3.5 Cloud Technology. The use of public or third party “cloud” technology to store / process / create Proprietary Information is authorized under the following conditions

3.3.5.1 only Software as a Service (SaaS) and other (GSM) cloud services will be used;

3.3.5.1.1 This contract’s Proprietary Information must not be stored using a third party cloud technology without additional demonstrated security controls implemented by the applicable Cloud Service Provider, as per the following government publications:

3.3.5.1.1.1 Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) (https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html)

3.3.5.1.1.2 Government of Canada Right Cloud Selection Guidance (https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-right-cloud-selection-guidance.html)

3.3.5.1.1.3 Government of Canada Cloud Security Risk Management Approach and Procedures (https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-security-risk-management-approach-procedures.html)

3.3.5.1.1.4 Government of Canada Security Control Profile for Cloud-Based GC Services (https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html)

3.3.5.1.1.5 Government of Canada Considerations for the Use of Cryptography in Commercial Cloud Services (https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-consideration-use-cryptography-in-cloud.html)

3.3.5.1.2 all aspects of the contractor's use of cloud computing and/or cloud technology must first be validated, assessed, and authorized by either the local department (DND DIM Secur) or Communications Security Establishment CSE (CCCS).

3.3.5.1.3 The Contractor must demonstrate that the measures comply with the requirements set forth in the following certifications and audit reports by providing upon request either independent third party assessment reports, certifications, or specific evidence of control implementation, that addresses the cloud service layer (e.g. IaaS, PaaS, SaaS) within the Cloud Service offering such as ; ISO/IEC 27001 or SOC 2 Type II and Self-assessment to Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

3.3.5.1.4 In addition to the above, the contractor must meet (or familiarize with) requirements outlined in PA Cloud IT Security Obligations Schedule 1.

3.3.6 Topology Diagram. A topology diagram of the IS 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 account (e.g. user, power user, event log reader, 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. !, $, #, %, etc.);

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:

3.4.3.2.1 must be changed at first login;

3.4.3.2.2 must be changed whenever there is any suspicion of compromise;

3.4.3.2.3 must not be the same as that user's password for any other Contract W6369-22-A009 Amendment 1 IS;

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

3.4.3.2.5 must 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.

3.4.3.4 Each time a local administrator password is changed it must be promulgated to all applicable personnel (e.g. IT support, system administrators, etc.) who must safeguard it commensurate with the highest sensitivity level of data processed on the system. It should 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 for which the password is used.

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; no removable media will be used in the IS for any data transfer for the contract W6369-22-A009 Amendment

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.

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 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:

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

3.5.5.2 the IT media's unique identifier;

3.5.5.3 the date and time it was removed from its GC-approved security container;

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

3.5.5.5 the date and time it was returned to its GC-approved security container; and

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

3.5.6 Air Gap Computer. The IS is not required to interact with untrusted sources (e.g. the internet, another network, removable IT media from another source, etc.) that would require the contractor to provide a standalone Air Gap computer.

**3.6 Document Printing and/or Reproduction**

3.6.1 Printing/Reproduction Authorization. The contractor is:

3.6.1.1 not 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

Use of either of these services to print and/or reproduce any Proprietary Information must first be approved 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. a different location unlikely to be affected by the same incident, such as a fire or flood, which could affect the primary location). 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 SOPs 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 Disposal of IT Media. Prior of the disposal of all IT media used under this contract - This includes for example, IT media that has failed, is being life cycled, is no longer required must follow the guidance in para 3.8.2 "IT Media Sanitization/Destruction". At the end of this contract, the disposal of IT media must be tracked via the use of a "Certificate of Destruction". The contractor must retain a copy of all IT disposal documents as evidence that the IT media has been properly disposed of. Destruction of classified information and assets must be recorded on a certificate of destruction form, a copy of which must be forwarded to PSPC's CSP by email at tpsgc.dgsssiprojetintl-dobissintlproject.pwgsc@tpsgc-pwgsc.gc.ca.

3.8.2 IT Media Sanitization/Destruction. The sanitization and destruction of all IT media on-site is <authorized> at the contractor's facility, under condition that the contractor must follow the sanitation and destruction guidance for high sensitivity media in accordance with CSE's "ITSP.40.006v2 - IT Media Sanitization" and the Contract Security Manual (CSM) Chap 6 "6.10 Destruction of records". The arrangements can be made with PSPC's CSP for IT Media disposal, if the contractor does not have the required means for IT media disposal.

3.8.3 Return of All Government Furnished Information/Material/Equipment (GFI/GFM/GFE). GFI/GFM/GFE will remain the property of DND, and must not be distributed outside the Contractor Team of this contract, unless approved by DND PO and at the end of the contract all GFI/GFM/GFE must be returned to the DND PO.

3.8.4 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.):

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

3.8.4.2 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.

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

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

**APPENDIX 3 TO ANNEX C – IT CLOUD SECURITY OBGLIGATIONS**

# For Protected A Cloud IT Security Obligations

## Schedule 1 to IT Security Requirements Document for Contract

## W6369-22-A009 Amendment 1

## 1. General

1.1 *Purpose*

The purpose of this Schedule is to set forth the obligations of the Contractor relating to the proper management of Department of National Defence's (DND)'s Data, including protection from unauthorized modification, access or exfiltration, in accordance with the Agreement, this Schedule, and the Contractor's Security Measures (collectively, the "**Security Obligations**") furthermore the contractor is expected to demonstrate that it continues to meet the same Security requirements and configuration that have been previously assessed and approved by CCCS.

This document outlines the Department of National Defence's (DND) Information Technology (IT) security requirements for the electronic processing, production, and/or storage of Canada's Data up to and including the level of PROTECTED A.

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. Contracted efforts should be preceded by the implementation of physical, personnel, procedural, information, and IT Security safeguards.

1.2 *Flow-Down of Security Obligations*

The obligations of the Contractor contained in these Security Obligations must be flowed down by the Contractor to any Sub-processors and/or Subcontractors to the extent applicable.

1.3 *Change Management*

The Contractor must, throughout the Contract, take all steps required to update and maintain the Security Requirements as needed to comply with the security best practices and industry standards.

The Contractor must advise DND of all changes that materially degrades or may have an adverse effect to the Cloud Services offerings in this Contract, including technological, administrative or other types of changes or improvements. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to GC.

## 2. Acknowledgments

The parties acknowledge that:

(a) DND's Data is subject to these Security Obligations.

(b) Notwithstanding any other provision of this Schedule, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to DND's Data.

(c) The Contractor must not have or attempt to gain custody of DND's Data, nor permit any Cloud Services Personnel to access DND's Data prior to the implementation of the Security Requirements as required under this Schedule on or before Contract Award.

(d) Security Obligations apply up to Protected A / Medium Integrity, Medium Availability or Medium Injury, unless otherwise specified.

**3. Securing Department of National Defence's (DND)'s Data**

(1) The Contractor must protect DND's Data from unauthorized access, modification, or exfiltration. This includes implementing and maintaining appropriate technical and organizational security measures including information security policies, procedures, and security controls to preserve the confidentiality, integrity, and availability of DND's Data.

**4. Roles and Responsibilities for Security**

(1) The Contractor must clearly delineate the roles and responsibilities for the security controls and features of the Cloud Services between the Contractor and DND PA. This includes, at a minimum, the roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system backup; (iv) incident management; (v) system monitoring; and (vi) vulnerability management.

(2) The Contractor must provide to DND an up-to-date document that delineates the roles and responsibilities: (i) at contract award; (ii) on an annual basis; (iii) when there are significant changes to such roles and responsibilities as a result of a Change to the Cloud Services; or (iv) upon request of DND PA.

**5. Third-Party Assurance: Certifications and Reports**

(1) The Contractor must ensure that DND's Data, Contractor Infrastructure (including any IaaS, PaaS or SaaS Service provided to GC) and Service Locations are secured with appropriate security measures that comply with the requirements set forth the Contractor's security practices and policies.

(2) The Contractor must demonstrate that the measures comply with the requirements set forth in the following certifications and audit reports by providing upon request either independent third party assessment reports, certifications, or specific evidence of control implementation, that addresses each service layer (e.g. IaaS, PaaS, SaaS) within the Cloud Service offering, including:

(a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body; or

(b) AICPA Service Organization Control (SOC) 2 Type II Audit Report 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality - issued by an independent Certified Public Accountant; and

(c) must do a Self-assessment to Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) using the latest version downloaded from https://cloudsecurityalliance.org/.

(3) Each certification, or audit report provided must: (i) identify the legal business name of the Contractor or applicable Sub-processor; (ii) identify the Contractor's or Sub-processor's certification date and the status of that certification; (iii) identify the services included

within the scope of the certification report. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

(4) Each audit, will result in the generation of an audit report which must be made available to DND. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor.

(5) Each SOC 2 Type II audit report must have been performed within the 12 months prior to the start of the contract. A bridge letter may be provided to demonstrate that the Contractor is in process of renewal where there is a gap between the service organization's report date and the user organization's year-end (i.e., calendar or fiscal year-end).

(6) The Contractor is expected to maintain the security controls supporting compliance with ISO 27001 or SOC 2 Type II for the duration of the contract. The Contractor must provide, at least annually, and promptly upon the request of DND PA, all reports, records or control implementation evidence that may be reasonably required to demonstrate that the Contractor's compliance or certifications are current and maintained.

(7) The Self-assessment to Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) must be made available to DND.

**6. Auditing Compliance**

(1) The Contractor must conduct the privacy and security audits of the security of the computers, computing environment and physical data centers that it uses in processing and protecting DND's Data as follows:

(a) Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

(b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

(c) Each audit will be performed by independent, third party auditors that (i) are qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conform to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

(2) Each audit will result in the generation of an audit report that must be made available to DND PA. The audit report must clearly disclose any material findings by the third party auditor. The Contractor must, at its own expense, promptly remediate issues and correct deficiencies raised in any audit report to the satisfaction of the auditor.

(3) Upon request of DND PA, additional supplementary evidence from the Contractor, including system security plans, designs, or architecture documents that provide a comprehensive system description, may be provided by the Contractor or a Sub-processor to supplement the certification and audit reports described in Section 5 (Third

Party Assurance) in order to demonstrate the Contractor's compliance with the required industry certifications.

**7. Cloud Service Provider (CSP) IT Security Assessment Program**

(1) The Contractor must comply with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services for Protected A, Medium Integrity and Medium Availability (PAMM) (https://www.canada.ca/en/government/system/digital-government/modern-emergingtechnologies/cloud-computing/government-canada-security-control-profile-cloud-based-itservices.html) for the scope of the Cloud Services provided by the Contractor. Compliance must be demonstrated upon request through the mapping of security controls to the applicable industry certifications identified below, and upon validated through independent third party assessments.

(2) Compliance will be assessed and validated periodically through the DND Security Program using the guidelines set by Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-serviceprovider-information-technology-security-assessment-process-itsm50100).

The Contractor must initiate the formal CCCS assessment process and commit to completing the program without undue delay. The contractor will provide the following documentation as they are made available:

(i) A copy of the confirmation letter that confirms that they have on-boarded into the program;
(ii) A copy of the most recent completed assessment report provided by CCCS; and
(iii) A copy of the most recent summary report provided by CCCS.

The Contractor should contact the CCCS Client Services for any additional information related to the CSP IT Assessment Program.

It is the continuous obligation of the Contractor of the proposed Cloud Services to notify DND PA and CCCS when there are significant changes to its delivery of the IT Security services supporting the Contractor offering.

**8. Data Protection**

(1) The Contractor must provide the capability to allow DND to:

(a) Implement encryption of data at rest for the Cloud Services hosting DND's Data where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, in accordance with Section 14 - Cryptographic Protection.

(b) Transmit DND's Data in a secure manner including ability for the GC and/or DND to implement encryption for data in transit for all transmissions of DND's Data, in accordance with Section 14 - Cryptographic Protection and Section 21- Network and Communications Security.

(2) The Contractor must:

(a) Implement security controls that restricts administrative access to DND's Data and Systems by the Contractor and provides the ability to require the approval of DND PA before the Contractor can access DND's Data to perform support, maintenance or operational activities.

(b) Take reasonable measures to ensure that Contractor Personnel do not have standing or ongoing access rights to DND's Data, and access is restricted to Contractor Personnel with a need-to-know, including resources that provide technical or DND support, based on approval from DND PA.

(3) The Contractor must not make any copies of databases or any part of those databases containing DND's Data outside of regular service resilience capabilities and within approved regional spaces or zones within Canada.

(4) The Contractor must not move or transmit approved copies outside of agreed upon service regions except when approval is obtained from DND PA.

(5) Upon request, the Contractor must provide DND PA with a document that describes all additional metadata created from DND's Data.

**9. Data Isolation**

(1) The Contractor must implement controls to ensure appropriate isolation of resources such that DND's Data are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Cloud Services and Contractor Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support:

(a) The separation between Contractor's internal administration from resources used by its customers;

(b) The separation of DND resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another; and

(c) Ability for the GC to support isolation within GC-managed tenant environment.

(2) Upon request of DND, the Contractor must provide DND PA with a document that describes the approach for ensuring appropriate isolation of resources such that DND's Data are not co-mingled with other tenant data, while in use, storage or transit.

**10. Data Location**

(1) The Contractor must have the ability to store and protect DND's Data, at rest, including data in backups or maintained for redundancy purposes. An approved Data Centre is defined as the following:

a. A data centre that meets all security requirements and certifications identified in Section 30 for Physical (Data Centre / Facilities) Security;

b. Ensures the infeasibility of finding a specific DND's data on physical media; and

c. Employs encryption to ensure that no data is written to disk in an unencrypted form, in accordance with Section 14 - Cryptographic Protection.

(2) The Contractor must certify that the delivery and provisioning of Cloud Services under this contract is:

a. from countries within the North Atlantic Treaty Organization (NATO) (https://www.nato.int/cps/en/natohq/nato_countries.htm); or

b. the European Union (EU) (https://europa.eu/european-union/about-eu/countries_en), or from countries with which DND has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(3) The Contractor can have the ability for DND to isolate DND's Data hosted in Cloud Services in data centers that are geographically located anywhere in Canada or outside of Canada.

(4) Upon request of DND, the Contractor must:

a. Provide the DND with an up-to-date list of the physical locations, including city, which may contain DND's Data for each data centre that will be used to provide the Cloud Services; and

b. Identify which portions of the Cloud Services are delivered from outside of Canada, including all locations where data is stored and processed and where the Contractor manages the service from.

(5) It is the continuous obligation of the Contractor of the proposed Cloud Services to notify DND when there are updates to the list of physical locations which may contain DND's Data.

## 11. Data Transfer and Retrieval

The Contractor must provide the capability including tools and services that allow DND to:

(a) Extract all online, nearline, and offline DND's Data, including, but not limited to, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a DND code repository, and network configurations such that DND can use these instructions to migrate from one environment to another environment; and

(b) Securely transfer all DND's Data, including content data and associated metadata, in a machine-readable and usable. In accordance with the Para 9 of the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/Pages/guidelines-file-formats-transferring-information-resources-enduring-value.aspx)

**12. IT media**

(1) Throughout the duration of this contract, all IT media used to process, produce and/or store unencrypted DND Information must be disposed in accordance with the Section 13 “Data Disposition and Returning”.

(2) In the event that equipment requires maintenance, support or replacement, **no IT media containing any DND 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) All IT media (e.g. internal hard drives, removable hard drives, external hard drives, CDs/DVDs, USB sticks, etc.) used to process, produce and/or store DND Information must:

(a) be dedicated to this contract only;

(b) be given a unique identifier to ensure positive control and tracking;

(c) be identified and inventoried by:

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

(ii) the information sensitivity level,

(iii) the release-ability caveat (if applicable), and

(iv) the model and serial number (if applicable);

(d) be labelled with:

(i) the highest sensitivity level of the data it contains,

(ii) the government department (in this case DND),

(iii) the contract number, and

(iv) the IT media's unique identifier.

(e) 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.).

(f) 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.

(g) 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:

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

(ii) the IT media's unique identifier;

(iii) the date and time it was removed;

(iv) the name or initials of the individual who signed it out;

(v) the date and time it was returned; and

(vi) the name or initials of the individual who returned the media.

**13. Data Disposition and Returning Records to Department of National Defence (DND)**

(1) Disposal of IT Media. Prior of the disposal of all IT media used under this contract - This includes for example, IT media that has failed, is being life cycled, is no longer required must follow the guidance in para (2) "IT Media Sanitization/Destruction". At the end of this contract, the disposal of IT media must be tracked via the use of a "Certificate of Destruction". The contractor must retain a copy of all IT disposal documents as evidence that the IT media has been properly disposed of. Destruction of classified information and assets must be recorded on a certificate of destruction form, a copy of which must be forwarded to PSPC's CSP by email at tpsgc.dgsssiprojetintl-dobissintlproject.pwgsc@tpsgc-pwgsc.gc.ca.

(2) IT Media Sanitization/Destruction. The sanitization and destruction of all IT media on-site is authorized at the contractor's facility, under condition that the contractor must follow the sanitation and destruction guidance for high sensitivity media in accordance with CSE's "ITSP.40.006v2 - IT Media Sanitization" and the Contract Security Manual (CSM) Chap 6 "6.10 Destruction of records".

(3) The arrangements can be made with PSPC's CSP for IT Media disposal, If the contractor does not have the required means for IT media disposal.

(4) Return of All Government Furnished Information/Material/Equipment (GFI/GFM/GFE). GFI/GFM/GFE will remain the property of DND, and must not be distributed outside the Contractor Team of this contract, unless approved by DND PO and at the end of the contract all GFI/GFM/GFE must be returned to the DND PO.

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

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

b. 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. 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 process, produce and/or store highly sensitive Proprietary

Information, the contractor must remove the volatile memory from the device and have it destroyed

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

**14. Cryptographic Protection**

The Contractor must:

(a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods;

(b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassifiedprotected-and-protected-b-information-itsp40111);

(c) Ensure that FIPS 140-2 or later validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://cyber.gc.ca/en/cryptographic-module-validation-program-cmvp) in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 or later validated cryptographic module is providing the expected security services in the expected manner; and

(d) Ensure that any FIPS 140-2 or later140-3 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.

**15. Key Management**

The Contractor must provide DND PA with a key management service that provides:

(a) Creation/generation and deletion of encryption keys by the GC;

(b) Definition and application of specific policies that control how keys can be used;

(c) Protection of access to the key material including prevention from Contractor access to the key material in unencrypted fashion;

(d) Ability to audit all events related to key management services, including Contractor access for GC's review;

(e) Ability to securely import GC generated keys from GC managed on-premise hardware security module (HSM) without exposure of key plaintext during the import process;

(f) Ability to prevent the Cloud Service Provider to recover plaintext copies of the GC generated keys; and

(g) Ability to delegate key use privileges for use by the Cloud Services used for the GC managed services.

**16. Endpoint Protection**

(1) The Contractor must implement, manage, and monitor security-hardened endpoints with active host-based protections to prevent against malware, attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or Certified Products from CSE (https://www.cyber.gc.ca/en/certified-products) or an equivalent standard approved by DND PA in writing.

(2) The Contractor must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO 27034, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by DND in writing. Upon request of DND, the Contractor must provide a document that describes the Contractor's documented software and system development lifecycle approach and process.

**17. Identity and Access Management**

(1) The Contractor must have the ability for DND to support secure access to Cloud Services including ability to configure:

(a) multi-factor authentication in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) using GC-approved credentials;

(b) Role-based access;

(c) Access controls on objects in storage; and

(d) Granular authorization policies to allow or limit access.

(2) The Contractor must have the ability to establish organization-wide defaults to manage tenant-wide policies.

**18. Federation**

(1) The Contractor must have the ability for DND to support federated identity integration including:

(a) Support for open standards for authentication protocols such as Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of DND; and

(b) Ability to associate DND unique identifiers (e.g. a DND unique ID, a DND email address, etc.) with the corresponding Cloud Service user account(s).

**19. Privileged Access Management**

(1) The Contractor must:

(a) Manage and monitor privileged access to the Cloud Services to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host DND services;

(b) Restrict and minimize access to the Cloud Services;

(c) Restrict DND's Data to only authorized devices and End users with an explicit need to have access;

(d) Enforce and audit authorizations for access to the Cloud Services and DND's Data;

(e) Constrain all access to service interfaces that host DND's Data to uniquely identified, authenticated and authorized DND, devices, and processes (or services);

(f) Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(g) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(h) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to DND's Data;

(i) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles;

(j) Adhere to the principles of least privilege and need-to-know when granting access to the Cloud Services and DND's Data;

(k) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint

that does not have Internet browsing or open e-mail access) to provide support and administration of Cloud Services and Contractor Infrastructure;

(l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and

(m) Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.

(2) The Contractor must provide to DND PA a document that describes the Contractor's approach and process for managing and monitoring privileged access of the Cloud Services.

**20. Remote Management**

(1) The Contractor must manage and monitor remote administration of the Contractor's Cloud Service that are used to host GC services and take reasonable measures to:

(a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(b) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions, in accordance with Section 14 (Cryptographic Protection);

(c) Route all remote access through controlled, monitored, and audited access control points;

(d) Expeditiously disconnect or disable unauthorized remote management or remote access connections; and

(e) Authorize remote execution of privileged commands and remote access to security-relevant information;

(2) The Contractor must provide to DND PA a document that describes the Contractor's approach and process for managing and monitoring remote administration of the Cloud Services.

**21. Network and Communications Security**

(1) The Contractor must:

(a) Provide the ability for GC to establish secure connections to the Cloud Services, including providing data-in-transit protection between DND and the Cloud Service using TLS 1.2, or subsequent versions;

(b) Use up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in CSE's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securelyconfiguring-network-protocols-itsp40062) and ITSP.40.111

(https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-andprotected-b-information-itsp40111);

(c) Use correctly configured certificates within the TLS connections in accordance with CSE guidance.

(d) Provide the ability for DND to implement network access controls and security rules that allow or deny network traffic to DND resources.

**22. Dedicated Connections**

(1) For IaaS layers, the Contractor must provide the ability for the GC to establish private redundant connectivity to the Cloud Services. This includes:

(a) Establishing connectivity either directly into the Defense Wide Area Network (DWAN) or in a GC-approved location within the geographic boundaries of Canada is not mandatory for protected A Cloud IS;

(b) Enabling full backup and disaster recovery services through redundant connections within and across Contractor data centers;

(c) Physical connectivity links that are optical, and that provide a minimum of 10 Gbps with the option to add additional links that provide up to 40 Gbps in aggregate, with optional 100 Gbps connectivity;

(d) Support for virtualization and multi-tenancy for all network components;

(e) Support for dynamic routing protocols (BGP) for all connections;

(f) Support for GC-approved protocols as outlined in:

i. ITSP.40.062 Guidance on Securely Configuring Network Protocols, Section 3.1 for AES cipher suites (https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062 )

ii. ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111)

(g) Provide a description of all the data centre locations where the capability is available.

**23. Logging and Auditing**

(1) The Contractor must implement log generation and management practices and controls for all Cloud Service components that store or process DND's Data, and that conform with industry standards and best practices, such as those found in NIST 800-92 (Guide to Computer Security Log Management), or an equivalent standard approved by DND in writing. Upon request of DND, the Contractor must provide a document that describes the Contractor's documented log generation and management practices and controls.

(2) The Contractor must provide the ability for DND to export security event logs for the Cloud Services it consumes, in support of GC operations including monitoring of the Cloud Services and for e-discovery and legal holds.

(3) The Contractor must enable DND to centrally review and analyze audit records from multiple components from the Cloud Services consumed by the DND. This includes the ability for DND to:

(a) log and detect audit events such as (i) successful and unsuccessful account login attempts, (ii) account management, (iii) object access and policy change, (iv) privilege functions and process tracking, (v) system events, (vi) deletion of data;

(b) record in logs (or log files) audit events that are time synchronized and timestamped in coordinated universal time (UTC) and protected from unauthorized access, modification, or deletion while in transit and at rest;

(c) separate Security Incidents and logs for different DND accounts to enable DND to monitor and manage events within its boundary that are affecting its instance of an IaaS, PaaS or SaaS Cloud Service provided to it by the Contractor or a Sub-processor; and

(d) forward DND tenant events and logs to a GC-managed centralized audit log system using standardized reporting interfaces, protocols, and data formats (e.g. Common Event Format (CEF), syslog, or other common log formats) and APIs that support log data remote retrieval (e.g. via a database interface using SQL, etc.).

(4) For SaaS, the Contractor must provide APIs that provide the ability to:

(a) Inspect and interrogate data at rest in SaaS applications;

(b) Assess events such as user access and behaviour, administrator access and behaviour, and changes to third-party API access, stored in SaaS application logs.

**24. Continuous Monitoring**

(1) The Contractor must continually manage, monitor, and maintain the security posture of Contractor Infrastructure and Service Locations hosting DND's Data throughout the contract, and ensure that the Cloud Services provided to DND are in a manner that complies with these Security Obligations. As part of this obligation, the Contractor must:

(a) Actively and continuously monitor threats and vulnerabilities to Contractor Infrastructure, Service Locations, or DND's Data;

(b) Undertake best efforts to prevent attacks through security measures such as denial of service protections;

(c) Undertake best efforts to detect attacks, Security Incidents, and other abnormal events;

(d) Identify unauthorized use and access of any Cloud Services, data and components relevant to DND's IaaS, PaaS or SaaS Cloud Service;

(e) Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the Cloud Services or libraries that the Cloud Services make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;

(f) Respond, contain, and recover from threats and attacks against the Contractor Cloud Services; and

(g) Where required, take proactive countermeasures, including taking both pre-emptive and responsive actions, to mitigate threats.

(2) The Contractor's Cloud Services must allow for GC application data (for IaaS, PaaS and SaaS) and GC network traffic (for IaaS and PaaS) of cloud hosted GC services to be copied and forwarded to a predetermined location (in the cloud or on GC premises).

(3) The Contractor's Cloud Services must allow GC to deploy and operate security software to perform advanced monitoring and mitigations of cyber threats for GC's Cloud Services at the GC managed host and network layer, for GC managed components only.

(4) On a frequency and schedule to be determined by the DND IT Security Authority, but with reasonable notice and within the constraints of applicable Privacy Laws and Regulations, DND retains the right to conduct inspections of every contractor's facility involved in this contract, including relevant sub-contracted infrastructure providers' facilities, 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.

**25. Security Incident Management**

(1) The Contractor's Security Incident response process for the Cloud Services must encompass IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities. This includes:

(a) A published and documented Security Incident Response Process for review by DND that is aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP800-612, Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/treasury-board-secretariat/services/accessinformation-privacy/security-identity-management/government-canada-cybersecurity-event-management-plan.html); or (iv) other best practices from industry standards, if DND determines, in its discretion, that they meet DND's security requirements;

(b) Documented processes and procedures of how the Contractor will identify, respond, remediate, report, and escalate Security Incidents to DND, including: (i) the scope of the information security incidents that the Contractor will report to

DND; (ii) the level of disclosure of the detection of information security incidents and the associated responses; (iii) the target timeframe in which notification of information security incidents will occur; (iv) the procedure for the notification of information security incidents; (v) contact information for the handling of issues relating to information security incidents; and (vi) any remedies that apply if certain information security occur;

(c) Ability for the Contractor to support DND's investigative efforts for any compromise of the users or data in the service that is identified;

(d) Allows only designated representatives of DND (e.g. SSC Security Operations Center) authorized by the Technical Authority:

(i) to request and receive discrete access and information associated with DND's Data (user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;

(ii) the ability for DND to track the status of a reported information security event.

(e) Procedures to respond to requests for potential digital evidence or other information from within the Cloud Services environment and includes forensic procedures and safeguards for the maintenance of a chain of custody.

(2) Upon request of DND, the Contractor must provide a document that describes the Contractor's Security Incident Response Process.

(3) The Contractor must:

(a) Work with DND's Security Operations Center(s) (e.g. CCCS, Departmental SOC) on Security Incident containment, eradication and recovery in accordance with the Security Incident Response process.

(b) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data or the service; and

(c) Track, or enable DND to track, disclosure of DND's Data, including what data has been disclosed, to whom, and at what time.

(5) DND may require forensic evidence from the Contractor to assist in a GC investigation. The Contractor agrees to provide assistance to the GC on a best effort basis.

**26. Security Incident Response**

(1) The Contractor must alert and promptly notify DND PA (via phone and email) of any compromise, breach or of any evidence such as (i) a security incident, (ii) a security malfunction in any asset, (iii) irregular or unauthorized access to any Asset, (iv) large scale copying of an Information Asset, or (v) another irregular activity identified by the

Contractor, that leads the Contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365 days), and will be made without undue delay, in any event, within 72 hours, and within the Contractor's service level commitments.

(2) If the Contractor becomes aware of and determines a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to DND's Data or Personal Data while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay (i) notify DND PA of the Security Incident; (ii) investigate the Security Incident and provide DND PA with detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the cause and to minimize any damage resulting from the Security Incident.

**27. Information Spillage**

(1) The Contractor must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, approved by DND PA in writing. Notwithstanding the foregoing, the Contractor's Information Spillage process must include, at a minimum:

(a) A process for identifying the specific data elements that is involved in a System's contamination;

(b) A process to isolate and eradicate a contaminated System; and

(c) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination.

(2) The Contractor must provide a document to the DND PA that describes the Contractor's Information Spillage Response Process.

**28. Security Testing and Validation**

(1) The Contractor must have a process that allows DND, upon request and under mutually accepted terms, to conduct a non-disruptive and non-destructive Vulnerability Scan or Penetration Test of DND's portion of the Cloud Service components within the Contractor environment.

(2) The Contractor must provide the ability to enable a self-service security health check, compliance or scoring tool that enables the measurement of the security posture of applicable Cloud Services leveraged for providing DND's services.

**29. Personnel Security Screening**

(1) All contractor personnel who have access to any DND's data must:

a. hold - at minimum - a valid reliability status which must be granted and be tracked by PSPC's CSP.

b. 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) No visitors, foreign nationals or unauthorized personnel shall have access to the DND's data, the Information system, or the zone where the DND's data is being processed, produced and/or stored unless they possess a valid reliability status and are escorted by an authorized contractor employee.

(3) The Contractor must implement security measures that grant and maintain the required level of security screening for Contractor Personnel engaged in the provision of the Cloud Services and for Sub-processor personnel pursuant to their access privileges to information system assets on which DND's Data is stored and processed.

(4) The Contractor screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbssct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by DND.

(5) Upon request of DND, the Contractor must provide a document that describes the Contractor's personnel security screening process. The process must provide, at a minimum:

(a) A description of the employee and Sub-processor positions that require access to DND's Data or have the ability to affect the confidentiality, integrity or availability of the Cloud Services;

(b) A description of the security screening activities and practices, including notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern;

(c) A description of the security awareness and training as part of employment onboarding, when employee and sub-processor roles change, and on an ongoing basis, to ensure that employees and Sub-processors understand, are aware of, and fulfil, their responsibilities for information security;

(d) A description of the process that is enforced when an employee or sub-processor changes their role or when employment is terminated;

(e) The approach to detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or effect on the reliability of Cloud Services hosting DND's data.

**30. Physical (Data Centre / Facilities) Security**

(1) Processing, production and/or storage of this contract's DND's data must only be performed in facilities which have been authorized by PSPC's CSP. All data must be processed, produced and/or stored in a secure manner that prevents unauthorized viewing, access, or manipulation.

(2) In accordance with the RCMP's "G1-026 Guide to the Application of Physical Security Zones", the IS (Information System) will be installed and operating in an Operation zone or in a temporary Operation zone.

(3) The Contractor must implement physical security measures that ensure the protection of IT facilities and information system assets on which DND's Data are stored and processed against all forms of tampering, loss, damage, and seizure. Physical protection of all facilities that host DND's Data, must be applied in accordance with, or use an adequate risk-based approach based on a prevent-detect-respond-recover approach to physical security, aligned with the physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (http://www.tbssct.gc.ca/pol/doc-eng.aspx?id=12329). The security measures required under this include, at a minimum:

(i) Sufficient redundancy and recovery capabilities within and between the Contractor's facilities including, being geographically disparate such that the loss of one facility does not prohibit recovery of data and DND's Data within the prescribed service level commitments;

(ii) Proper handling of IT Media;

(iii) Controlled maintenance of all information systems and their components to protect their integrity and ensure their ongoing availability;

(iv) Controlled access to information system output devices to prevent unauthorized access to DND's Data;

(v) Limiting physical access to DND's Data and Service Locations to authorized Cloud Services Personnel based on position or role and the need-to-access principle, and validated by two forms of identification;

(vi) Enforcing safeguarding measures for DND's data at alternate work sites (e.g., telework sites); and

(vii) Recording and monitoring all physical access to Service Locations and all logical access to Systems hosting DND's Data, using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.

(4) The Contractor must provide a document to DND PA that describes the Contractor's physical security measures.

(5) If any physical security measures is to change in a way that materially degrades the physical security, the Contractor must inform the DND PA.

**31. Supply Chain Risk Management**

(1) The Contractor must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide Cloud Services. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least privilege access for all personnel within the supply chain.

(2) The Contractor must have a supply chain risk management approach including a Supply Chain Risk Management Plan that is aligned with one of the following best practices:

(i) ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4);

(ii) NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or

(iii) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan.

(3) Within 90 days of contract award, the Contractor must:

(a) Provide proof that the SRCM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA DND, and/or ISO certification regime

OR

(b) Provide DND with a copy of the SRCM Plan on an annual basis, or upon request of DND.

(4) In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with the Section 31 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS provider using a GC-approved IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a supply chain integrity (SCSI) review. This SCSI review will be conducted no sooner than every three years.

**32. Industrial Security Program – Security Requirement for Canadian Suppliers**

(1) The Contractor must, at all times during the performance of the Contract/Standing Offer/Supply Arrangement, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED A, issued by the Industrial Organization Security Services Directorate (OSS), **Public Services and Procurement Canada (PSPC).**

(2) The Contractor MUST NOT utilize its Information systems to electronically process, produce or store PROTECTED information until written approval has been issued by the client department security authority. After approval has been granted, these tasks may be performed at the level of PROTECTED A including an IT Link at the level of PROTECTED A.

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

(a) Security Requirements Check List and security guide (if applicable);

(b) Industrial Security Manual (Latest Edition);

(c) OSS website: Security requirements for contracting with the Government of DND, located at www.tpsgc-pwgsc.gc.ca/esc-src

**NOTE:** There are multiple levels of personnel security screenings associated with this file. In this instance, a security guide must be added to the SRCL clarifying these screenings. The security guide is normally generated by the organization's project authority and/or security authority.

**33. Industrial Security Program – Security Requirements for Foreign Suppliers**

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in DND is the Industrial Security Sector (ISS), Public Services and Procurement Canada (PSPC), administered by International Industrial Security Directorate (IISD), PSPC. The Canadian DSA is the authority for confirming **Contractor/Subcontractor** compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient **Contractor/Subcontractor** incorporated or authorized to do business in a jurisdiction other than DND and delivering/performing outside of DND for the Cloud Services described in the Cloud Solution, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified in the Section entitled Protection and Security of Data Stored in Databases.

(1) The **Contractor/Subcontractor** certifies that the delivery and provisioning of Cloud Services under the terms of this contract must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which DND has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(2) The Foreign recipient **Contractor/Subcontractor** must at all times during the performance of the **contract/subcontract** be registered with the appropriate government administered supervisory authority in the country(ies) in which it is incorporated or operating and authorized to do business. The Foreign recipient **Contractor/Subcontractor** must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and the Canadian DSA.

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

(a) Foreign recipient **Contractor/Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

(b) The Foreign recipient **Contractor/Sub-processor/Subcontractor** must identify an authorized Contract Security Officer (CSO) and an Alternate Contract Security Officer (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in this contract. This individual will be appointed by the proponent foreign recipient **Contractor's/Subcontractor'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.

(c) The **Contractor/Subcontractor** must not grant access to **DND PROTECTED** information/assets, except to personnel who have a need-to-know for the performance of the **contract** and have been screened in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbssct.gc.ca/pol/doc-eng.aspx?id=28115), or use acceptable equivalent measures agreed to by DND.

(d) **DND PROTECTED** information/assets, provided to the foreign recipient **Contractor/Subcontractor** or produced by the Foreign recipient **Contractor /Subcontractor**, must:

i. not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **contract**, without the prior written consent of DND. Such consent must be sought from the Canadian DSA in collaboration with the Contracting Authority; and

ii. not be used for any purpose other than for the performance of the **contract** without the prior written approval DND. This approval must be obtained by contacting the Contracting Authority (in collaboration with the Canadian DSA).

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

(5) The Foreign recipient **Contractor /Subcontractor** must not use the **DND PROTECTED** information/assets for any purpose other than for the performance of the **contract** without the prior written approval of the Government of DND. This approval must be obtained from the Canadian DSA.

(6) The Foreign recipient **Contractor/Subcontractor** must, at all times during the performance of the **contract** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **DND PROTECTED**.

DND has the right to reject any request made separate and apart from the authorization in this Contract in connection with the Contractor delivering Cloud Services to electronically access, process, produce, transmit or store **DND PROTECTED** data related to the Cloud Services in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

National Defence
National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

**APPENDIX 4 TO ANNEX C – AIR GAP COMPUTER DOCUMENT**

# Department of National Defence (DND)

## Air Gap Computer Document

## for

## Contract W6369-22-A009 Amendment 1

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

## 1. Introduction

**1.1** This document outlines the Information Technology (IT) security requirements for Department of National Defence (DND) Contract W6369-22-A009 Amendment 1 for the transfer of electronic information between the Information System (IS) - identified herein for this document only as the IS - used to store / process / create this contract's Proprietary Information up to and including the level of Protected A. The scope of this "Air Gap Computer Document for Contract W6369-22-A009 Amendment 1 is to state the minimum IT security requirements necessary to transfer electronic information to and from the IS.

**1.2** 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 Public Services and Procurement Canada Contract Security Program (PSPC/CSP).

**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 IS 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 store / process / create information up to and including Protected A. Validation must be provided by PSPC/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 IS 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 IS. |
| 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.<br><br>For the IS the type(s) of Source Transfer Media will be USB stick 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 Contract W6369-22-A009 Amendment 1 Air Gap Computer to the Target System.<br><br>For the IS the type(s) of Target Transfer Media will be USB stick as well as any other type(s) of removable media approved in writing by the DND Project Authority. |

### 2.3 Hardware

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

2.3.2 This Air Gap Computer must be owned by the contractor and be installed, configured, and operational before being inspected by PSPC/CSP.

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

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 IS is installed.

2.3.6 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.

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

2.3.7.1 the highest sensitivity level of the data it contains,

2.3.7.2 the government department (in this case DND),

2.3.7.3 the contract number (in this case W6369-22-A009 Amendment 1),

2.3.7.4 the IT media's unique identifier, as discussed in para 3.5.3.2 of the "IT Security Requirements Document for Contract W6369-22-A009 Amendment 1, and

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

2.3.8 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.).

2.3.9 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 "IT Security Requirements Document for Contract W6369-22-A009 Amendment 1. 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 "IT Security Requirements Document for Contract W6369-22-A009 Amendment 1.

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 contract's Air Gap Computer, and all items specified in the paragraph "Logging and Auditing" of the "IT Security Requirements Document for Contract W6369-22-A009 Amendment 1 must be followed.

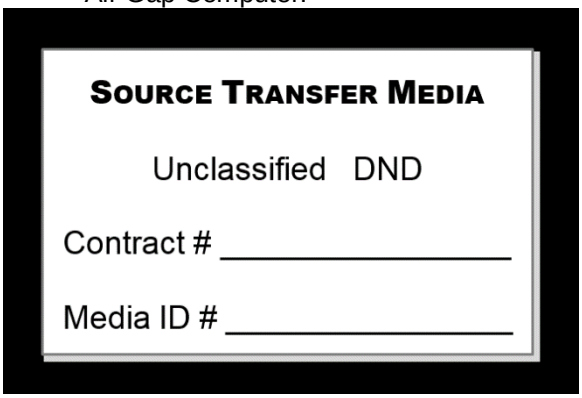
2.4.5 All accounts on this contract's Air Gap Computer must follow the applicable sections of the paragraph "Authorization and Access Control" of the "IT Security Requirements Document for Contract W6369-22-A009 Amendment 1. No shared or generic accounts are authorized.

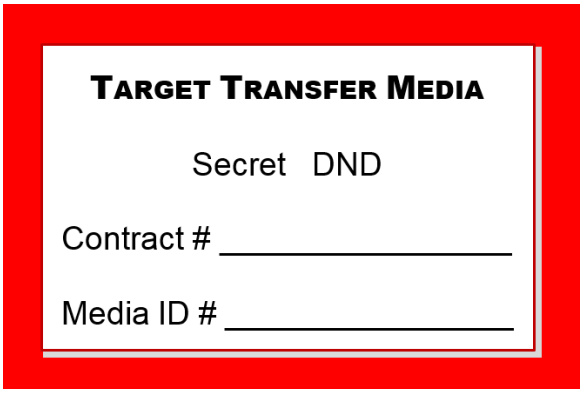
2.4.6 The following paragraphs of the "IT Security Requirements Document for Contract W6369-22-A009 Amendment 1 are applicable to this Air Gap Computer and must be followed:

- "Information at Rest";
- "IT Media"; and
- "Disposal".

**2.5 Air Gap Computer and SOP**

2.5.1 The IS SOP must include the procedures and details mentioned in this "Air Gap Computer Document for Contract W6369-22-A009 Amendment 1 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 Contract W6369-22-A009 Amendment 1 Air Gap Computer.

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

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

## DATA TRANSFER PROCEDURES

1. Power on the Contract W6369-22-A009 Amendment 1 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.