

**RETURN BIDS TO :****RETOURNER LES  
SOUMISSIONS À:**[Alexander.cormierhowie@sac-isc.gc.ca](mailto:Alexander.cormierhowie@sac-isc.gc.ca)**REQUEST FOR PROPOSAL  
DEMANDE DE PROPOSITION****Proposal To:** Indigenous Services Canada

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

**Proposition aux:** Services aux  
Autochtones Canada

Nous offrons par la présente de vendre Sa Majesté le Roi en droit du Canada du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexées, au(x) prix indiqué(s).

**Instructions :** See Herein**Comments - Commentaires****Ce document contient une sécurité  
Exigence - This document contains a  
Security  
Requirement**

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

**Issuing Office – Bureau de distribution**  
Indigenous Services Canada/ Services aux  
Autochtones Canada

<b>Title – Sujet</b> NATIONAL NURSE SCHEDULER (NNS)	
<b>Solicitation No. – N° de l'invitation</b> 1000254069	<b>Date</b> February 22 <sup>nd</sup> , 2024
<b>Client Reference No. – N° référence du client</b> N/A	
<b>GETS Reference No. – N° de reference de SEAG</b>	
<b>File No. – N° de dossier</b> N/A	<b>CCC No. / N° CCC - FMS No. / N° VME</b> N/A
<b>Solicitation Closes – L'invitation prend fin</b> <b>at – à 02 :00 PM</b> <b>on – le April 2<sup>nd</sup>, 2024</b>	<b>Time Zone</b> Fuseau horaire EST
<b>F.O.B. - F.A.B.</b> <b>Plant-Usine: Y Destination: Y Other-Autre: Y</b>	
<b>Address Inquiries to : - Adresser toutes questions à:</b> <a href="mailto:Alexander.cormierhowie@sac-isc.gc.ca">Alexander.cormierhowie@sac-isc.gc.ca</a>	<b>Buyer Id – Id de l'acheteur</b> DY6
<b>Telephone No. – N° de téléphone :</b> 873-354-0959	<b>FAX No. – N° de FAX</b> N/A
<b>Destination – of Goods, Services, and Construction:</b> <b>Destination – des biens, services et construction :</b>  Ontario	

**Instructions: Voir aux présentes**

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

## TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION.....	3
1.1 SECURITY REQUIREMENTS .....	3
1.2 STATEMENT OF WORK.....	3
1.3 DEBRIEFINGS.....	3
PART 2 - BIDDER INSTRUCTIONS.....	4
2.1 STANDARD INSTRUCTIONS, CLAUSES AND CONDITIONS.....	4
2.2 SUBMISSION OF BIDS.....	4
2.3 FORMER PUBLIC SERVANT.....	4
2.4 ENQUIRIES - BID SOLICITATION.....	5
2.5 APPLICABLE LAWS.....	6
PART 3 - BID PREPARATION INSTRUCTIONS.....	7
3.1 BID PREPARATION INSTRUCTIONS .....	7
PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION.....	8
4.1 EVALUATION PROCEDURES.....	8
4.1.1 TECHNICAL EVALUATION .....	8
4.1.1.1 MANDATORY TECHNICAL CRITERIA.....	8
4.1.1.2 POINT RATED TECHNICAL CRITERIA.....	11
4.2 BASIS OF SELECTION.....	13
PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION .....	14
5.1 CERTIFICATIONS REQUIRED WITH THE BID.....	15
5.2 CERTIFICATIONS PRECEDENT TO CONTRACT AWARD AND ADDITIONAL INFORMATION .....	15
PART 6 - RESULTING CONTRACT CLAUSES.....	15
6.1 SECURITY REQUIREMENTS .....	17
6.2 STATEMENT OF WORK.....	18
6.3 STANDARD CLAUSES AND CONDITIONS.....	18
6.4 TERM OF THE CONTRACT .....	19
6.5 AUTHORITIES .....	19
6.6 PROACTIVE DISCLOSURE OF CONTRACTS WITH FORMER PUBLIC SERVANTS .....	20
6.7 PAYMENT .....	20
6.8 INVOICING INSTRUCTIONS .....	21
6.9 CERTIFICATIONS AND ADDITIONAL INFORMATION.....	21
6.10 APPLICABLE LAWS.....	21
6.11 PRIORITY OF DOCUMENTS .....	21
ANNEX "A" .....	22
STATEMENT OF WORK .....	22
ANNEX "B" .....	46
BASIS OF PAYMENT .....	46
ANNEX "C" .....	48
SECURITY REQUIREMENTS CHECK LIST .....	48

## **PART 1 - GENERAL INFORMATION**

### **1.1 Security Requirements**

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.

### **1.2 Statement of Work**

The Work to be performed is detailed under Annex A of the resulting contract clauses.

### **1.3 Debriefings**

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**

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 Manual](https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) (<https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual>) issued by Public Works and Government Services Canada.

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.

The [2003](#) 2020-05-28 Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 5.4 of [2003](#), Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days

Insert: 90 days

### **2.2 Submission of Bids**

Bids must be submitted electronically only to Indigenous Services Canada (ISC) by the date, time and e-mail address indicated on page 1 of the bid solicitation.

Due to the nature of the bid solicitation, bids transmitted by any other means to ISC will not be accepted.

### **2.3 Former Public Servant**

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPSs, bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

#### **Definitions**

For the purposes of this clause, "former public servant" is any former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

an individual;

an individual who has incorporated;

a partnership made of former public servants; or

a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act*, 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11, the *Members of Parliament Retiring Allowances Act*, R.S. 1985, c. M-5, and that portion of pension payable to the **Canada Pension Plan Act, R.S., 1985, c. C-8.**

#### **Former Public Servant in Receipt of a Pension**

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes ( ) No ( )**

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:

name of former public servant;

date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2019-01 and the Guidelines on the Proactive Disclosure of Contracts.

#### **Work Force Adjustment Directive**

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes ( ) No ( )**

If so, the Bidder must provide the following information:

name of former public servant;

conditions of the lump sum payment incentive;

date of termination of employment;

amount of lump sum payment;

rate of pay on which lump sum payment is based;

period of lump sum payment including start date, end date and number of weeks;

number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

## **2.4 Enquiries - Bid Solicitation**

All enquiries must be submitted in writing to the Contracting Authority no later than 3 calendar days before the bid closing date. Enquiries received after that time may not be answered.

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.

## **2.5 Applicable Laws**

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

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.

## **PART 3 - BID PREPARATION INSTRUCTIONS**

### **3.1 Bid Preparation Instructions**

Canada requests that the Bidder submits its bid electronically in accordance with section 8 of the 2003 standard instructions and as amended in Part 2 - Bidder Instructions, Article 2.1 Standard Instructions, Clauses and Conditions. Bidders are required to provide their bid in a single transmission. The total size of the email, including all attachments, must not exceed 10 megabytes (MB). It is solely the Bidder's responsibility to ensure that the total size of the email does not exceed this limit.

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

- Section I: Technical Bid
- Section II: Financial Bid
- Section III: Certifications
- Section IV: Additional Information

#### **Section I: Technical Bid**

In their technical bid, Bidders should explain and demonstrate how they propose to meet the requirements and how they will carry out the Work.

#### **Section II: Financial Bid**

Bidders must submit their financial bid in accordance with the Basis of Payment.

##### **3.1.1 Electronic Payment of Invoices – Bid**

The method of invoice payment by Indigenous Services Canada (ISC) is by direct deposit to the Contractor's financial institution of choice.

## **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 and financial evaluation 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**

Bids must meet the Mandatory Technical Criteria specified below. The Bidder must provide the necessary documentation, as indicated, to support compliance with each Mandatory Technical Criterion.

Bids which fail to meet the Mandatory Technical Criteria will be declared non-responsive. Each Mandatory Technical Criterion should be addressed separately.

The following definitions apply to the Technical Evaluation Criteria for this RFP:

Business Administrators - A User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements of Annex A – Statement of Work.

Contract Health Care Professionals - A non-Indigenous Services Canada employed Registered Nurse, Nurse Practitioner, Licensed Practical Nurse, Registered Practical Nurse, Primary Care Paramedic, Advanced Care Paramedic, Critical Care Paramedic, and/ or other designations of professional providing health-related services to Indigenous Peoples.

Data Team - A User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements of Annex A – Statement of Work.

Health Care Professionals (HCPs) - A Registered Nurse, Nurse Practitioner, Licensed Practical Nurse, Registered Practical Nurse, Primary Care Paramedic, Advanced Care Paramedic, Critical Care Paramedic, and/ or other designations of professional providing health-related services to Indigenous Peoples, and whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements of Annex A – Statement of Work.

Health Facilities - A (Indigenous Services Canada - ISC/ First Nations and Inuit Health Branch - FNIHB) healthcare facility within which primary care and public health services are delivered (e.g., nursing station, health centre with or without treatment, hospital).

Nurse In Charge (NIC) - A User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements of Annex A – Statement of Work.

Nurse Management - A User of NNS who is an (Acting) Nurse Manager whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements of Annex A – Statement of Work.

Schedulers - A User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements of Annex A – Statement of Work.

Travel Team - A User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements of Annex A – Statement of Work.



User(s) - A person and/ or group who uses NNS.

<b>Mandatory Technical Criteria (MT)</b>		
<b>Number</b>	<b>Mandatory Technical Criterion (MT)</b>	<b>Bid Preparation Instructions</b>
<b>MT1</b>	<p>The Bidder must have a minimum of 5 continuous years of experience in the delivery of scheduling systems that support the complex scheduling of a variety of professionals, with varying designations, in numerous (geographical) locations.</p> <p>The experience must have been acquired within five years of the solicitation closing date.</p>	<p>The Bidder must provide the following information:</p> <ol style="list-style-type: none"> <li>1. Certificate of Compliance;</li> <li>2. Procurement Business Number (PBN); and,</li> <li>3. Documentation confirming these requirements.</li> </ol>
<b>MT2</b>	<p>The Bidder must provide a system that complies with, or can be modified to comply with, the Official Languages Act (<a href="https://laws-lois.justice.gc.ca/eng/acts/O-3.01/index.html">https://laws-lois.justice.gc.ca/eng/acts/O-3.01/index.html</a>) by being functionally equivalent in English and French and must allow Users to work in the Canadian official language of their choice.</p>	<p>The Bidder must provide the following information:</p> <p>Documentation, including screenshots, or similar visualization(s), confirming this requirement.</p>
<b>MT3</b>	<p>The Bidder must provide a system that enables up to 100 Business Administrators, Schedulers and Travel Team members to add and/ or edit data concurrently without performance degradation.</p>	<p>The Bidder must provide the following information:</p> <p>Documentation confirming this requirement.</p>
<b>MT4</b>	<p>The Bidder must provide a system that enables up to 3000 HCPs to be concurrently logged in and viewing their schedules (read-only ability) without performance degradation.</p>	<p>The Bidder must provide the following information:</p> <p>Documentation confirming this requirement.</p>
<b>MT5</b>	<p>The Bidder must provide a User Guide (for the system) accessible from within the Graphical User Interface (GUI) in both official languages (English and French). The User Guide must provide step-by-step instructions on how to complete all User tasks.</p> <p>The Bidder must provide a system that automatically notifies Users of any modifications to the features and functionality of the system.</p> <p>The Bidder must immediately provide updates to the User Guide when any modifications are made to the system.</p>	<p>The Bidder must provide the following information:</p> <p>Documentation, including screenshots, or similar visualization(s), confirming this requirement.</p>
<b>MT6</b>	<p>The Bidder must provide a system that has the ability to “toggle” between multiple schedule views (e.g., 1 week, 1 month, 3 months, etc.) and filter specific date ranges.</p>	<p>The Bidder must provide the following information:</p> <p>Documentation, including</p>

		screenshots, or similar visualization(s), confirming this requirement.
<b>MT7</b>	The Bidder must provide a system that ensures real-time update tracking/ status.	The Bidder must provide the following information:  Documentation, including time-stamped screenshots, or similar visualization(s), confirming this requirement.
<b>MT8</b>	The Bidder must provide a system using cloud-based technology (i.e., without being connected to the ISC network) and is accessible on mobile devices (e.g., tablets, smartphones, android devices, iPhones) and laptop/ desktop computers.	The Bidder must provide the following information:  Documentation confirming this requirement.
<b>MT9</b>	The Bidder must provide a system that is able to authenticate User access using multifactor authentication, for designated Users.	The Bidder must provide the following information:  Documentation confirming this requirement.
<b>MT10</b>	The Bidder must provide a system capable of performing comprehensive analytics and generating (parametrized) comparison, historical and operational reports using all available or selected fields.  The system's reporting requirements must include, but not be limited to: <ul style="list-style-type: none"> <li>• Generate ad hoc reports, identifying results of traces made;</li> <li>• Build a data mart for corporate reports;</li> <li>• Create administrative reports; and,</li> <li>• Schedule recurring reports to designated individuals by email or notification in the system.</li> </ul>	The Bidder must provide the following information:  Documentation, including screenshots, copies of reports, or similar visualization(s), confirming this requirement.
<b>MT11</b>	The Bidder must provide a system that has extensive search and filtering capabilities.	The Bidder must provide the following information:  Documentation, including screenshots or similar visualization(s), confirming this requirement.
<b>MT12</b>	The Bidder must provide a system that allows numerous and various types/ designations of Users, each with unique and clearly defined functionality.	The Bidder must provide the following information:  Documentation, including screenshots or similar visualization(s), confirming this requirement.
<b>MT13</b>	The Bidder must provide a system that incorporates effective visual mechanisms (e.g. colour coding) in order to: <ul style="list-style-type: none"> <li>• Distinguish between HCP designations so that a Scheduler/ Nurse Management can quickly determine the allocation of (varying) HCPs in Health Facilities (e.g., Contract vs ISC, NP, RN,</li> </ul>	The Bidder must provide the following information:  Documentation, including screenshots or similar visualization(s), confirming this requirement.

	<p>LPN, NIC, paramedics (PCP, ACP, CCP), etc.).</p> <ul style="list-style-type: none"> <li>• Provide simplistic views on a community's current and future staffing levels (based on ideal requirements) – e.g., understaffed = red / meets requirements = green / overstaffed = blue.</li> <li>• Provide simplistic views of an HCP's availability (e.g., available = green, already scheduled = blue, vacation = orange, etc.).</li> </ul>	
<b>MT14</b>	<p>The Bidder must provide a system that enables designated Users the ability to input and edit scheduling information, including but not limited to the following:</p> <ul style="list-style-type: none"> <li>• Regular rotation/ shift</li> <li>• Illness</li> <li>• Travel</li> <li>• Vacation</li> <li>• Orientation</li> <li>• Training</li> <li>• Telework</li> </ul> <p>The system must incorporate effective visual mechanisms (e.g. colour coding) in order to differentiate the (above) scheduling categories (available from a configurable dropdown list).</p>	<p>The Bidder must provide the following information:</p> <p>Documentation, including screenshots or similar visualization(s), confirming this requirement.</p>

#### 4.1.1.2 Point Rated Technical Criteria

Bids meeting all the Mandatory Technical Criteria will be evaluated and scored as specified in the tables inserted below.

Bids must achieve a minimum of 5 points for each of the four unique criteria, and a minimum total of 30 points for the combined score of the four criteria.

Bids that fail to obtain the required minimum number of points specified will be declared non-responsive. Each point-rated technical criterion should be addressed separately.

Point Rated Technical Requirements (PRT)		Bid Preparation Instructions	Weighting (Points)	
<b>PRT1</b>	The Bidder should have a comprehensive bilingual (French and English) training plan, based on User needs, to ensure ease of use and learning of the system.	The Bidder must provide an example of its comprehensive bilingual (French and English) training plan, specific to NNS, which details step-by-step instructions on how to complete all User tasks.	0 points	Bidder does not have a bilingual (French and English) training plan.
			5 points	Bidder has a standard universal bilingual (French and English) training plan.
			10 points	Bidder has a customizable bilingual

				(French and English) training plan specific to all NNS User types.
<b>PRT2</b>	The Bidder should provide ongoing bilingual (French and English) support services for training, as needed.	The Bidder must provide documentation outlining its ongoing bilingual (French and English) training support services, including how NNS Users can request support, available communication channels and the expected timelines for response and resolution.	0 points	Bidder does not offer ongoing bilingual (French and English) training support services.
			5 points	Bidder offers ongoing bilingual (French and English) training support services with limitations (e.g., fixed monthly frequency) and/ or lacks clarity on support/ communication channels.
			10 points	Bidder offers ongoing bilingual (French and English) training support services as needed and clearly demonstrates the support, communication channels, and expected timelines for response and resolution.
<b>PRT3</b>	The Bidder should provide a detailed pre-implementation plan covering the pre-implementation phase, from the date of contract award to the implementation date, to perform all activities defined in the Statement of Work.	The Bidder must provide a pre-implementation plan which includes the following requirements: <ul style="list-style-type: none"> <li>• A detailed list of all tasks to be completed.</li> <li>• An explanation or rationale for each task.</li> <li>• A Responsibility Assignment Matrix (RAM) outlining the participation required from the Bidder and the Project Authority for task completion.</li> <li>• Any dependencies where Canada's involvement is required.</li> </ul>	0 points	No pre-implementation plan is provided, or the plan does not include all listed requirements.
			5 points	The pre-implementation plan includes all listed minimum requirements but lacks comprehensive details, clear explanations, or key elements.
			10 points	The pre-implementation plan includes all listed minimum requirements that demonstrate a comprehensive understanding of the project.

<b>PRT4</b>	The Bidder should have a comprehensive business continuity and disaster recovery plan.	The Bidder must provide documentation explaining its business continuity and disaster recovery plan specifying its strategy for managing NNS scheduling data.  This must include: <ul style="list-style-type: none"> <li>• Details on how backup documents are stored.</li> <li>• The frequency of backup.</li> <li>• Measures to ensure data integrity during the backup process.</li> </ul>	0 points	Business continuity and disaster recovery plan are not provided.
			5 points	The business continuity and disaster recovery plan are non-comprehensive and/ or lacks details in explanation.
			10 points	A comprehensive business continuity and disaster recovery plan providing a clear strategy for NNS scheduling data.
<b>Maximum Available Points = 40</b>				
<b>Minimum Overall Points Required = 30</b>				

#### 4.2 Basis of Selection

1. To be declared responsive, a bid must:
  - a. comply with all the requirements of the bid solicitation; and
  - b. meet all mandatory criteria; and
  - c. obtain the required minimum points specified for the technical evaluation, and
  - d. obtain the required minimum of 30 points overall for the technical evaluation criteria which are subject to point rating.  
The rating is performed on a scale of 40 points.
2. Bids not meeting (a) or (b) or (c) and (d) will be declared non-responsive.
3. The selection will be based on the highest responsive combined rating of technical merit and price. The ratio will be 70 % for the technical merit and 30% for the price.
4. To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows: total number of points obtained / maximum number of points available multiplied by the ratio of 70 %.
5. To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 30 %.
6. For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.

7. Neither the responsive bid obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive bid with the highest combined rating of technical merit and price will be recommended for award of a contract.

The table below illustrates an example

Where all three bids are responsive and the selection of the contractor is determined by a 70/30 ratio of technical merit and price, respectively. The total available points equals 135 and the lowest evaluated price is \$45,000 (45).

**Basis of Selection - Highest Combined Rating Technical Merit (70%) and Price (30%)**

		Bidder 1	Bidder 2	Bidder 3
<b>Overall Technical Score</b>		115/135	89/135	92/135
<b>Bid Evaluated Price</b>		\$55,000.00	\$50,000.00	\$45,000.00
<b>Calculations</b>	<b>Technical Merit Score</b>	$115/135 \times 70 = 59.63$	$89/135 \times 70 = 46.15$	$92/135 \times 70 = 47.70$
	<b>Pricing Score</b>	$45/55 \times 30 = 24.55$	$45/50 \times 30 = 27$	$45/45 \times 30 = 30$
<b>Combined Rating</b>		84.18	76.15	77.70
<b>Overall Rating</b>		1st	3rd	2nd

**PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION**

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

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.

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**

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

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

In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide with their bid, **if applicable**, the declaration form available on the [Forms for the Integrity Regime](http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html) 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**

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 provided will render the bid non-responsive.

### **5.2.1 Integrity Provisions – Required Documentation**

In accordance with the section titled Information to be provided when bidding, contracting or entering into a real procurement agreement of the [Ineligibility and Suspension Policy](http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html) (<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.

## **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's proposed individuals requiring access to classified or protected information, assets or sensitive work sites must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;
  - (c) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites;
  - (d) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;
  - (e) 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. Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.
  3. For additional information on security requirements, Bidders should refer to the [Contract Security Program](http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) 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.



## 7.1 Security Requirements

7.1.1 The following security requirement exists for this contract:

### **SECURITY CLAUSES: 1000254069**

1. Pursuant to the Policy on Government Security, the nature of the services to be provided under this contract requires a valid Government of Canada (GoC) personnel Security Screening at the level of **Reliability Status** for the Contractor, authorized resources and any sub-contractors to be assigned to conduct the work.
2. Prior to the commencement of the work, the Contractor and each authorized resources involved in the performance of the work under this contract must each hold a valid Security Screening at the level of **Reliability Status** during the lifetime of the contract.
3. The Contractor and its personnel requiring access to PROTECTED information, assets or sensitive work site(s) must EACH hold a valid Security Screening at the level of **Reliability Status**.
4. The Contractor **MUST NOT** possess or safeguard **PROTECTED** information/assets at their organization's premises until the Security In Contracting team of Indigenous Services Canada (ISC) receives a signed copy of the contract. After the contract has been granted and we receive a signed copy, these tasks may be performed up to the level of **Protected A**.
5. The Contractor **MUST NOT** remove any **Sensitive** information from the identified work site(s), and the Contractor must ensure that its personnel are made aware of and comply with this restrictions.
6. The Contractor **MUST NOT** utilize its Information Technology (IT) systems to electronically process, produce or store any sensitive information until the Security In Contracting of Indigenous Services Canada (ISC) team receives a signed copy of the contract. After contract has been granted and we receive a copy, these tasks may be performed up to the level of **Protected A**
7. Subcontracts are not to be awarded without the prior written permission from the security in contracting team of ISC.
8. Any substitute or alternate resource proposed for this contract:
  - a) must be approved by the Security and Emergency Services Divisions of Indigenous Services Canada; and,
  - b) must hold a valid GoC Security Screening at the level of **Reliability Status**, before gaining access to designated information or assets.
9. Under this contract, if a Contractor submits a resource who is subsequently found to not meet the Security requirements, the Department may immediately terminate the contract with no obligation to replace the resource with a resource from the same Contractor or to pay any invoice for work undertaken by this resource.
10. This contract only has force or effect for as long as the Security Screening at the level of **Reliability Status** is valid. During the lifetime of this contract, if the Security Screening issued prior to the commencement of the work, be suspended or revoked the contract shall be terminated immediately and the Contractor shall have no claim against Her Majesty or the Minister as a result of the termination. The Contractor shall be paid for satisfactory work performed up to the time of termination pursuant to the terms of the Contract.
11. The Contractor must comply with the provisions of the:
  - a) Security Requirements Agreement, attached as Annex D; and

- b) Policy on Government Security <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578>

#### 7.1.1.1 Safeguarding Measures

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

- 7.1.1.2 The Contractor must provide the services of the following person(s) to perform the Work as stated in the Contract:

### 7.2 Statement of Work

The Work to be performed is detailed under Annex "A" of the resulting contract clauses.

### 7.3 Standard Clauses and Conditions

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

#### 7.3.1 General Conditions

**2010B** 2020-05-28 General Conditions - Professional Services (Medium Complexity) apply to and form part of the Contract with the following adaptations:

- a) References to Public Works and Government Services Canada (PWGSC) are replaced by the Indigenous Services Canada (ISC); and
- b) Section 10, Subsection 1 is amended as follows:
  - Delete: "Invoices must be submitted in the Contractor's name. The Contractor must submit invoices for each delivery or shipment; invoices must only apply to the Contract. Each invoice must indicate whether it covers partial or final delivery."
  - Insert: "Invoices must be submitted by Email to the Project Authority in the Contractor's name. The Contractor must submit invoices for each delivery or shipment; invoices must only apply to the Contract. Each invoice must indicate whether it covers partial or final delivery."
- c) Section 10, Subsection 2, paragraph a. is amended as follows:
  - Delete: "the date, the name and address of the client department, item or reference numbers, deliverable/description of the Work, contract number, Client Reference Number (CRN), Procurement Business Number (PBN), and financial code(s)"
  - Insert: "the contract title and number, the date, deliverable/description of the Work and financial code(s)"
- d) Insert: "2010B 36 (2018-05-10) Liability  
The Contractor is liable for any damage caused by the Contractor, its employees, subcontractors, or agents to Canada or any third party. Canada is liable for any damage caused by Canada, its employees or agents to the Contractor or any third party. The Parties agree that no limitation of liability or indemnity provision applies to the Contract unless it is specifically

incorporated in full text in the Articles of Agreement. Damage includes any injury to persons (including injury resulting in death) or loss of or damage to property (including real property) caused as a result of or during the performance of the Contract.”

## **7.4 Term of the Contract**

### **7.4.1 Period of the Contract**

The period of the Contract is 4 years from contract award.

### **7.4.3 Option to Extend the Contract**

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 2 additional 1 year period(s) under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least 5 calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

## **7.5 Authorities**

### **7.5.1 Contracting Authority**

The Contracting Authority for the Contract is:

Name: Alex Cormier Howie  
Title: Senior Procurement Officer  
Indigenous Services Canada  
Materiel and Assets Management Directorate  
Address: 10 rue Wellington, 13<sup>th</sup> floor, Gatineau, Qc, K1A 0H4

Telephone: 873-354-0959  
E-mail address: [alexander.cormierhowie@sac-isc.gc.ca](mailto:alexander.cormierhowie@sac-isc.gc.ca)

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 Project Authority**

The Project Authority for the Contract is:

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Organization: \_\_\_\_\_  
Address: \_\_\_\_\_

Telephone: \_\_\_\_\_  
Facsimile: \_\_\_\_\_  
E-mail address: \_\_\_\_\_

The Project 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 Project Authority, however the Project 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**

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Organization: \_\_\_\_\_  
Address: \_\_\_\_\_

Telephone: \_\_\_\_\_  
Facsimile: \_\_\_\_\_  
E-mail address: \_\_\_\_\_

### **7.6 Proactive Disclosure of Contracts with Former Public Servants**

By providing information on its status, with respect to being a former public servant in receipt of a [Public Service Superannuation Act](#) (PSSA) pension, the Contractor has agreed that this information will be reported on departmental websites as part of the published proactive disclosure reports, in accordance with [Contracting Policy Notice: 2019-01](#) of the Treasury Board Secretariat of Canada.

### **7.7 Payment**

#### **7.7.1 Basis of Payment**

#### **7.7.2 Limitation of Expenditure**

Canada's total liability to the Contractor under the Contract must not exceed \$ \_\_\_\_\_. Customs duties are excluded and Applicable Taxes are extra.

No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

when it is 75% committed, or

four months before the contract expiry date, or

as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

whichever comes first.

If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

#### **7.7.5 Electronic Payment of Invoices – Contract**

The method of invoice payment by Indigenous Services Canada (ISC) is by direct deposit to the Contractor's financial institution of choice.

If not registered for direct deposit payments, to enable payment, the Contractor must complete the Indigenous Services Canada Electronic Payment Request form ([http://www.aadnc-aandc.gc.ca/DAM/DAM-INTER-HQ/STAGING/texte-text/20\\_545\\_1362495227097\\_eng.pdf](http://www.aadnc-aandc.gc.ca/DAM/DAM-INTER-HQ/STAGING/texte-text/20_545_1362495227097_eng.pdf)), and submit the form to the address provided.

## **7.8 Invoicing Instructions**

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. Invoices must be distributed as follows:

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

## **7.9 Certifications and Additional Information**

### **7.9.1 Compliance**

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.

## **7.10 Applicable Laws**

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

## **7.11 Priority of Documents**

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

- (a) the Articles of Agreement;
- (b) the general conditions 2020-05-28 General conditions: Professional services (medium complexity)
- (c) Annex A, Statement of Work;
- (d) Annex B, Basis of Payment;
- (e) Annex C, Security Requirements Check List;
- (f) the Contractor's bid dated \_\_\_\_\_.

## **ANNEX "A"**

### **STATEMENT OF WORK**

#### **NATIONAL NURSE SCHEDULER (NNS)**

##### **1. SCOPE**

###### **1.1. Introduction**

Indigenous Services Canada (ISC) has a requirement for a contractor to provide a national electronic scheduling system (National Nurse Scheduler – NNS) for Health Care Professionals (HCPs) providing services in (the predominantly northern) communities in which First Nations and Inuit Health Branch (FNIHB) provides primary and public health care.

###### **1.2. Objectives of the Requirement**

The objective of the contract is to ensure that ISC obtains an NNS that is secure, bilingual (English and French) and accessible to all pertinent FNIHB staff that are essential in ensuring that HCPs, with the required qualifications, are scheduled and present, in the Health Facilities when needed.

One of the mandates of ISC, FNIHB is to improve access to high-quality services and the well-being of Indigenous Peoples in communities across Canada. FNIHB is also mandated to ensure the availability of, or access to, health care services for Indigenous communities.

In order to achieve this, FNIHB requires an NNS (utilized by Alberta, Manitoba, Ontario, and Quebec regions, and Nursing Relief Coordination Unit-NRCU) for HCPs providing services in northern communities. Based on departmental/ operational requirements, Saskatchewan and Atlantic regions may also be included in the scope of this project.

In addition to enhancing ISC, FNIHB's ability to deliver its mandate, NNS will allow ISC to be more agile and responsive to patient care by optimizing the workforce in a cost-effective manner. As well, NNS must have the ability to perform analytics and generate comparison(s), historical and operational reports.

NNS will be pivotal in supporting the provision of safe and quality health care services in Health Facilities by ensuring the right staff are deployed to the correct location at the right time. The importance of HCPs and clinical staff to have ongoing access to a national, easy-to-use scheduling system cannot be overemphasized, and will be achieved with the deployment of NNS. This aligns with the following principles within the Departmental Results Framework:

- Health/ Departmental Result 3 – Indigenous Peoples have access to quality federally-funded health services; and,

- Children and families/ Departmental Result 4 – Indigenous Peoples are culturally safe and socially well.

Key stakeholders (of NNS) include:

- HCPs - who provide services at Health Facilities and would rely on NNS for their itinerary;
- Nurse Management/ Nurses-in-Charge (NICs)/ Schedulers - who perform clinical and management-related responsibilities and schedule the HCPs;
- Data Team - who need to produce regular and required staffing reports;
- Travel Team - who enter HCP travel arrangements into NNS and make changes as needed;
- FNIHB (senior management) - who need to ensure that the FNIHB mandate is delivered; and,
- Indigenous Peoples/ clients - whom FNIHB provides health care services to.

The scope, or work, that is required to complete this procurement/ project includes the following stages:

- Acquisition (of NNS);
- Training;
- Implementation;
- Migration;
- Development;
- Testing;
- Phased-in/ agile “Go Live”; and,
- Continued support/ technical assistance and guidance.

### **1.3. Background and Specific Scope of the Requirement**

ISC funds and/ or delivers primary care services, accessible on a twenty-four hours a day, seven days a week (24/7) basis in over 50 Health Facilities serving approximately 111,000 First Nations clients in remote, semi-isolated and isolated First Nations communities, where access to provincial services is limited or non-existent. As of May 2022, this care is provided by approximately 269 full-time equivalent positions and delivered by approximately 390 nursing personnel.

Primary and public health care is considered a mandatory or an essential service under ISC’s program mandate, as it has a direct impact on the health and safety of individuals and the population. In these communities, HCPs working out of Health Facilities are often the only health service(s) providers. HCPs work in pairs or small groups, often with little to no support from other medical professionals, providing services to respond to urgent community health care needs and medical emergencies whenever they arise.

ISC is committed to both closing the gaps in health outcomes between Aboriginal and non-Aboriginal communities as indicated in the Truth and Reconciliation’s 94 Calls to Action as well as the [Accessible Canada Act](#) target to achieve a barrier-free Canada. ISC will continue to strive to ensure compliance with these objectives by engaging with our partners to offer primary

health services through a client-centered approach, ensuring that services are available to community members in a manner that facilitates access to all.

Maintaining consistent HCP staffing across Health Facilities is crucial to ensuring the delivery of high-quality health care services. Inconsistency, or any irregularities, in the scheduling of HCPs presents a serious risk to patient safety, exponentially increased by the ongoing HCP shortages across Canada.

Expected business outcomes following the deployment of NNS include:

- FNIHB (senior management) are able to deliver on their mandate;
- (NNS) Users will have the ability to perform complex scheduling of HCPs in Indigenous communities and also to study trends, including the ability to report on HCP shortages and gaps in FNIHB's ability to provide necessary services;
- HCPs will have a secure and easy access to a national electronic scheduling system in order to access their itinerary;
- FNIHB's data team are able to generate accurate staffing reports and;
- Indigenous Peoples, and their communities are able to access health care as and when needed.

## 2. REQUIREMENTS

### 2.1. Tasks, Activities, Deliverables and Milestones

NNS system requirements are divided into four sections: Business Requirements (Table 2.1.1.), Functional Requirements (Table 2.1.2.), Non-functional Requirements (Table 2.1.3.) and Technical Scalability Requirements (Table 2.2.1.).

Table 2.1.1. Business Requirements (BR) of NNS

Reference #	Business Requirement	Priority
BR-001	System must provide a centralized scheduling system, able to support complex scheduling of HCPs, of varying designations, across all applicable regions (Alberta, Manitoba, Ontario and Quebec), their communities and the individual Health Facilities.  Based on departmental/ operational requirements, Saskatchewan and Atlantic regions may also be included in the scope of this project.	Must Have
BR-002	System must address the challenges of scheduling HCPs in and between multiple locations/ communities in the regions.	Must Have
BR-003	System must be accessible to, but not be limited to, the following Users:	Must Have



	<ul style="list-style-type: none"> <li>• HCPs</li> <li>• Schedulers (regional, NRCU and Locum &amp; Travel Nurse Team)</li> <li>• Nurse Management <ul style="list-style-type: none"> <li>✓ Nurse(s) in Charge (NIC)</li> <li>✓ Nurse Practice Team</li> </ul> </li> <li>• Data Team</li> <li>• Travel Team</li> <li>• Business Administrators</li> </ul> <p>Note: The system will not be accessible to contractors and Contract HCPs.</p>	
BR-004	System must provide real-time update tracking/ status, have the ability to perform analytics and generate comparison, historical and operational reports.	Must Have
BR-005	System must store, and provide accurate HCP information including, but not limited to: <ul style="list-style-type: none"> <li>• Surname</li> <li>• Given name(s)</li> <li>• Phone # (work and personal)</li> <li>• Email address (work and personal)</li> <li>• Home address</li> <li>• Preferred spoken language (French or English)</li> <li>• Date of hire</li> <li>• Date of birth</li> <li>• Education</li> <li>• Licensing</li> <li>• Insurance</li> <li>• Training</li> <li>• Skill level</li> </ul>	Must Have
BR-006	System must be deployable using cloud-based technology (i.e., without being connected to ISC network), and is accessible on mobile devices (e.g., tablets, smartphones, android devices, iPhones) as well as laptop/ desktop computers.	Must Have
BR-007	System must have the ability to view/ report/ identify current and future staffing of HCPs (based on requirements) for all Health Facilities/ communities – with the goal that at a quick glance, a User could see HCP staffing levels, and the designations of HCPs..	Must Have

BR-008	System must have the ability to import/ migrate information/ data from existing systems including, but not limited to, UKG/ Kronos Workforce Dimensions scheduling system and MS Excel.	Must Have
BR-009	System must have access to (contractor provided) bilingual (French and English) subject matter expert (SME) support, by phone, with a response time of 30 minutes or less, Monday to Friday between the business hours of 07:00 – 20:00 EST.	Must Have
BR-010	System should have access to 24/ 7/ 365 (contractor provided) bilingual (French and English) subject matter expert (SME) support, by phone, with a response time of 30 minutes or less.	Should Have
BR-011	System must be user-friendly and intuitive.	Must Have
BR-012	System must be capable of interfacing with existing ISC reporting tools (i.e., Cognos Analytics, SQL, Power BI).	Must Have
BR-013	System must have the ability to integrate with MS Outlook (Office 16 and above) to schedule and send reports.	Must Have
BR-014	System must manage/ protect/ secure Protected A data.	Must Have
BR-015	System must have the ability to capture notes associated with schedules.	Must Have
BR-016	System must have the ability to generate parametrized auditing functions including, but not limited to, audit tracking log reporting, allowing filtering for specific periods, and /or User.	Must Have
BR-017	System must allow “READ Access” and privileges to the ISC Data Base Administrative (DBA) team to perform the required data extraction and/ or duplication from the system database into the (ISC) departmental infrastructure premises.	Must Have

Table 2.1.2. Functional Requirements (FR) of NNS

Reference #	Functional Requirement	Priority
FR-001	System must provide the ability to add, and configure, various types/ designations of Users.  User types/ designations will include,	Must Have

	but not be limited to, Business Administrators, Schedulers, Data Team, Travel Team, Nurse Management, and HCPs – each type/ designation must have a configurable functionality.	
FR-002	<p>System must allow Business Administrators to perform the following functions, including but not limited to:</p> <p><u>Human Element</u></p> <ul style="list-style-type: none"> <li>• Add new User(s)</li> <li>• Select or create a role for new User(s)</li> <li>• Select or create unique or multiple regions for new User</li> <li>• Edit User information</li> <li>• Reset User password</li> <li>• Deactivate User</li> </ul> <p><u>Scheduling Element</u></p> <ul style="list-style-type: none"> <li>• Enter HCP assignment timeslots into the system and make changes as needed.</li> </ul> <p><u>Administrative Element</u></p> <ul style="list-style-type: none"> <li>• Edit preset scheduling options</li> <li>• Add/ remove communities, regions, etc., to the business structure</li> <li>• Edit custom reports</li> </ul>	Must Have
FR-003	<p>System must allow Schedulers to perform the following functions, including but not limited to:</p> <p><u>Human Element</u></p> <ul style="list-style-type: none"> <li>• Add new User(s)</li> <li>• Select or create a role for new User(s)</li> <li>• Select or create unique or multiple regions for new User</li> <li>• Add/ edit scheduling constraints (e.g., stop work orders, certifications, etc.)</li> <li>• Edit User information</li> <li>• Reset User password</li> <li>• Deactivate User</li> </ul> <p><u>Scheduling Element</u></p> <ul style="list-style-type: none"> <li>• Enter HCP assignment timeslots</li> </ul>	Must Have

	into the system and makes changes as needed.	
FR-004	<p>System must allow the Data Team to perform the following functions, including but not limited to:</p> <p><u>Human Element</u></p> <ul style="list-style-type: none"> <li>View User(s) information</li> </ul> <p><u>Scheduling Element</u></p> <ul style="list-style-type: none"> <li>Access to reports and data</li> <li>Ability to review and create standard and ad hoc reports</li> </ul>	Must Have
FR-005	<p>System must allow the Travel Team to perform the following functions, including but not limited to:</p> <p><u>Scheduling Element</u></p> <ul style="list-style-type: none"> <li>Enter HCP travel arrangements into the system and make changes as needed</li> </ul>	Must Have
FR-006	<p>System must allow Nurse Management to perform the following functions, including but not limited to:</p> <p><u>Human Element</u> (View Only/ No Editing Functionality)</p> <ul style="list-style-type: none"> <li>View User(s) information</li> </ul> <p><u>Scheduling Element</u> (View Only/ No Editing Functionality)</p> <ul style="list-style-type: none"> <li>View HCP schedules based on (need to know) access</li> </ul>	Must Have
FR-007	<p>System must allow HCPs to perform the following functions, including but not limited to:</p> <p><u>Scheduling Element</u> (View Only/ No Editing Functionality)</p> <ul style="list-style-type: none"> <li>View their past, present and future schedule</li> </ul>	Must Have
FR-008	System must provide the ability to add, and configure, Health Facilities (and communities) in Alberta, Manitoba, Ontario, Québec, Saskatchewan and Atlantic (regions)	Must Have
FR-009	System must allow designated Users the ability to input and edit scheduling	Must Have

	<p>information including, but not limited to the following:</p> <ul style="list-style-type: none"> <li>• Regular rotation/ shift;</li> <li>• Illness;</li> <li>• Travel</li> <li>• Vacation;</li> <li>• Orientation;</li> <li>• Training; and,</li> <li>• Telework.</li> </ul> <p>The system must incorporate effective visual mechanisms (e.g., colour coding) in order to differentiate the (above) scheduling categories (available from a configurable dropdown list).</p>	
FR-010	System must have highly configurable parameters – i.e., designed to maximize flexibility by making system values user-configurable instead of embedding them in the code.	Must Have
FR-011	System must allow Business Administrators and Schedulers to view the audit trail (e.g., what Users are accessing the system, number of login attempts, etc.).	Must Have
FR-012	<p>System must have the ability to perform comprehensive analytics and generate (parameterized) comparison, historical and operational reports using all available or selected fields.</p> <p>Reporting requirements include, but are not to be limited to:</p> <ul style="list-style-type: none"> <li>• Generate ad hoc reports; identifying results of traces made;</li> <li>• Build a data mart for corporate reports;</li> <li>• Create administrative reports; and,</li> <li>• Schedule recurring reports to designated individuals by email or notification in the system.</li> </ul>	Must Have
FR-013	System must provide optimum performance related to the time to generate reports (i.e., time to generate (extensive) return data/ reports is less than 10 minutes).	Must Have

FR-014	System must have the ability to export all reports via a variety of methods (e.g., to csv, .xlsx, PDF).	Must Have
FR-015	System must only allow access to Users who have logged in with a unique username and password.	Must Have
FR-016	System must enforce strong passwords (e.g., minimum length, combination of alpha, numeric and special characters as per Government of Canada standards).	Must Have
FR-017	System must enable a User who has forgotten their unique username and password, a User driven method to obtain their unique username and change their password.	Must Have
FR-018	System must lock any User account after a predefined number of failed login attempts.	Must Have
FR-019	System must be able to authenticate User access using multifactor authentication, for designated Users.	Must Have
FR-020	System should have the ability to display an alert indicator associated with a scheduled HCP with a mandatory certification that has either expired or is going to expire in 3 months.	Should Have
FR-021	System should have the ability to display an alert indicator associated with an HCP's restrictions related to a band council resolution and/ or stop work order.	Should Have
FR-022	System must incorporate effective visual mechanisms (e.g., colour coding) in order to: <ul style="list-style-type: none"> <li>• Distinguish between HCP designations so that a Scheduler/ Nurse Management could quickly determine the allocation of (varying) HCPs in Health Facilities (e.g., Contract vs ISC, NP, RN, LPN, NIC, paramedics (PCP, ACP, CCP), etc.).</li> <li>• Provide simplistic views on a community's current and future staffing levels (based on ideal requirements) – e.g., under staffed = red / meets requirements = green / over-</li> </ul>	Must Have

	<p>staffed = blue.</p> <ul style="list-style-type: none"> <li>• Provide simplistic views of a HCP's availability (e.g., available = green, already scheduled = blue, vacation = orange, etc.)</li> </ul>	
FR-023	System should auto-assign a unique identifier to each User.	Should Have
FR-024	System must have the ability to upload documents (e.g., emails, PDF, Word documents, JPEG) with a file size limit up to 12 MB. These documents would include, but not be limited to: <ul style="list-style-type: none"> <li>• Travel itineraries (original and amended, if applicable) from ISC or Contract HCPs</li> <li>• Emails indicating ground transportation requirements</li> </ul>	Must Have
FR-025	System must allow Health Facilities to have unique hours of operation, a variable number of shifts, and the ability to schedule HCPs into customizable time-slots.	Must Have
FR-026	System user interface must be designed to identify and efficiently complete the most frequent User tasks - e.g., by prepopulating the most frequently used fields (e.g., HCP names and designations, community/ Health Facility names, etc.).	Must Have
FR-027	System must provide a simple, intuitive and common-sense method of scheduling HCPs, and editing schedules.	Must Have
FR-028	System must have extensive search and filtering capabilities.	Must Have
FR-029	System must allow Users to access a variety of menu items that include, but are not limited to: <ul style="list-style-type: none"> <li>• HCP "master";</li> <li>• Travel coordination;</li> <li>• Each unique Health Facility; and,</li> <li>• HCP profiles.</li> </ul>	Must Have
FR-030	System must have a feature that differentiates between pending (User) leave/ vacation not yet approved, and leave that has been approved (no longer pending).	Must Have
FR-031	System must have the ability to "toggle" between multiple schedule views (e.g.,	Must Have

	1 week, 1 month, 3 months, etc.) and be able to filter specific date ranges.	
FR-032	System must allow Users, based on defined functionality, to view (and edit, if applicable) all past, present and future HCP assignment timeslots that have been entered/ populated (in the system).	Must Have
FR-033	System must prompt Users with “do you want to save your changes” (or similar prompt) after making edits and be equipped with a prominent refresh icon to incorporate recent changes.	Must have
FR-034	System must be able to associate travel schedules and travel documents (e.g., PDF) to an HCP scheduled to work in a Health Facility, and incorporate travel updates (e.g., flight, or other modes of transportation, delays or cancellations) so that the latest travel information (added or edited in the system by a User) is available (and first to be viewed by User), but also allow past/ recent travel information to be available.  System must also prompt an alert indicator when there have been any changes to an HCPs travel. The prompt could be a “paperclip attachment” incorporating updates changes to travel.	Must Have
FR-035	System must allow the User to easily access, via the System screen/ image, a legend that defines the effective visual mechanisms (e.g., colour coding) utilized for/ to meet FR-009 and FR-022.	Must Have
FR-036	System must provide a robust and well documented method for a secure and controlled environment for data exchange, such as an Application Programming Interface (API). This method must protect sensitive information and minimize the risk of unauthorized access without compromising performance or stability.	Must Have

Table 2.1.3. Non-functional Requirements (NFR) of NNS

Reference #	Non-functional Requirement	Priority
NFR-001	System must be available to all Users 24 hours a day, 7 days a week, 365 days a	Must Have



	<p>year (24/ 7/ 365).</p> <p>System must enable a “simple view” of scheduling information for the continuity of scheduling if system maintenance, updates, etc. occur between 07:00 – 20:00 EST.</p>	
NFR-002	<p>System must comply with, or can be modified to comply with, the Official Languages Act (<a href="https://laws-lois.justice.gc.ca/eng/acts/O-3.01/index.html">https://laws-lois.justice.gc.ca/eng/acts/O-3.01/index.html</a>), by being functionally equivalent in English and French, and must allow Users to work in the Canadian official language of their choice.</p>	Must Have
NFR-003	<p>System must include a User Guide, accessible from within the Graphical User Interface (GUI) in both official languages (English and French). The User Guide must provide step-by-step instructions on how to complete all User tasks.</p> <p>User Guides must be in a format that enables the User to print.</p> <p>In addition, the system must automatically notify Users of any modifications to the features and functionality of the system.</p> <p>The User Guide must be updated immediately when any modifications have been made to the system.</p>	Must Have
NFR-004	<p>System must respond to (User) commands within 3 seconds under normal operating conditions and provide notification for responses that take longer.</p>	Must Have
NFR-005	<p>System should have the ability to automatically notify one or many groups (of Users), or individual Users, when Health Facility (HCP) staffing is, or will be, less than the minimum staffing requirements.</p> <p>Note: requirements will include up to three unique HCP factors</p>	Should Have
NFR-006	<p>System should integrate with multiple</p>	Should Have

	identity and credential providers using Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) protocols.	
NFR-007	The system must provide a web-based GUI with secured communication with the backend system.	Must Have
NFR-008	System must, in the event of a failure, be capable of restoring all data saved prior to the point of failure.	Must Have
NFR-009	System must implement a session time-out and auto-logoff functionality for (specific) inactive Users. The time-out value must be a configurable system-wide parameter.	Must Have
NFR-010	System must be deployable using cloud-based technology (i.e., without being connected to ISC network).	Must Have
NFR-011	System must adhere to Government of Canada information management requirements (e.g., retention period, disposition).	Must Have
NFR-012	System must prompt the appropriate Scheduler(s) and Business Administrator when an HCP (User) has been inactive for 6 months, or a timeframe that is configurable by selected Users.	Must Have
NFR-013	System must host and store all data in Canada at all times.	Must Have
NFR-014	System must meet all applicable ISC/ CIRNAC security and privacy requirements as outlined in: <ul style="list-style-type: none"> <li>• Annex B_Schedule 1_Security Obligations; and,</li> <li>• Annex B_Schedule 2_Privacy Obligations</li> </ul>	Must Have
NFR-015	System must be compliant with the following Government of Canada Web standards: <ul style="list-style-type: none"> <li>• Standard on Web Accessibility <a href="https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=23601">https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=23601</a></li> <li>• Standard on Web Usability (including common layouts) <a href="https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=24227">https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=24227</a></li> <li>• Standard on Web Interoperability <a href="https://www.tbs-">https://www.tbs-</a></li> </ul>	Must Have

	<p><a href="https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=25875">sct.canada.ca/pol/doc-eng.aspx?id=25875</a></p> <ul style="list-style-type: none"> <li>• Standard on Optimizing Websites and Applications for Mobile Devices <a href="https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=27088">https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=27088</a></li> <li>• Policy on Service and Digital <a href="https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603">https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603</a></li> <li>• Directive on Service and Digital <a href="https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601">https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601</a></li> <li>• Directive on Automated Decision-Making <a href="https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592">https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592</a></li> </ul>	
--	---	--

Table 2.1.4. Deliverables of NNS

Note<sup>1</sup>: All Deliverables in Table 2.1.4. must be available in both official languages (French and English)

Note<sup>2</sup>: All Deliverables in Table 2.1.4. must be Free on Board (FOB) ISC, or ISC designated destination

Note<sup>3</sup>: All Meetings in Table 2.1.4. will be virtual

Note<sup>4</sup>: All Documents in Table 2.1.5. must be MS (Microsoft) or MS-compatible

Deliverable Title	Deliverable Description	Deliverable Method/ Type	Deliverable Due Date
Meeting(s) Plan: <ul style="list-style-type: none"> <li>• Project kick-off meeting(s); and,</li> <li>• Regular project meetings</li> </ul>	The contractor must lead/ chair a project kick-off meeting(s) as well as regular project meetings in which discussions and agreements will take place related to how the project will be implemented, (listed) deliverables and the schedule.  The kick-off meeting should occur no later than 10 business days after contract signing.	Meetings; and, Documents (including, but not limited to, a contractor developed workplan based on the delivery of the work (Statement of Work)	Within 20 business days, after contract signing (by all parties)
(Initial) Training Plan	The contractor must provide an (initial) plan which ensures that the training is comprehensive enough so that ISC trainees	Documents (including, but not limited to, (Initial) Training Plan)	Within 40 business days, after contract signing (by all

	<p>are, at a minimum, enabled, to:</p> <ul style="list-style-type: none"> <li>• Use all functional and administrative features; and,</li> <li>• Configure and tune the features as necessary.</li> </ul> <p>The contractor must propose the best, and the alternative methods, of providing training, with respect to the location of trainees in Alberta, Saskatchewan, Manitoba, Ontario, Quebec and Atlantic Region.</p>		parties)
Communication Plan	The contractor must provide a plan outlining the process(es) of how communications and engagement will effectively occur between Project Authority, Technical Authority and contractor, including descriptions on points of contact, frequency, and methodologies.	Documents (including, but not limited to, Communication Plan)	Within 40 business days, after contract signing (by all parties)
Implementation Plan	<p>The contractor must provide a plan which describes how, and when, the contractor envisages all activities; pertinent to implementation, not limited to the following:</p> <ul style="list-style-type: none"> <li>• Creation of various environments (i.e., scheduling test/ sandbox)</li> <li>• Creation of system access for the Users, and applicable functionality;</li> <li>• Configuration and tuning of system;</li> <li>• Design and implementation of workflow templates and business processes, as needed; and,</li> <li>• Re-configuration and re-tuning of system based on lessons learned.</li> </ul>	Documents (including, but not limited to, Implementation Plan)	Within 40 business days, after contract signing (by all parties)
(Core) Training	Guided by the (Initial) Training	Professional	Within 60

Plan	Plan, the contractor will provide a plan to train up to 100 core Users, which would enable them to perform functional and performance testing as well as general use of the system.	Services; and, Documents (including, but not limited to, (Core) Training Plan)	business days, after contract signing (by all parties)
Testing Plan - Functional and Performance	<p>The contractor must provide a plan which outlines:</p> <ul style="list-style-type: none"> <li>Set up and use of testing/ sandbox environments for functional and performance testing</li> </ul> <p>The contractor must be available to ISC, and assist if required, in troubleshooting the functional and performance testing of the system.</p>	Professional Services; and, Documents (including, but not limited to, Testing Plan - Functional and Performance)	Within 60 business days, after contract signing (by all parties)
User Guides	<p>The contractor must provide unique User Guides that outline all functional and usage requirements for all User categories.</p> <p>The User Guides must be updated immediately when any modifications have been made to the system.</p>	Documents (including, but not limited to, User Guides)	Within 60 business days, after contract signing (by all parties)
Security Requirements	As a part of the Security Assessment and Authorization (SA&A) process that the contractor must fully participate in, evidence must be properly documented information of a high quality that clearly and unambiguously demonstrates that the security controls (ITSG-33) have been properly implemented, configured and are operating correctly to secure the system.	Documents	Within 60 business days, after contract signing (by all parties)
Go Live	The contractor must support ISC, as required, when the system goes live, as per the defined project schedule.	Professional Services	As necessary
Post Go Live	The contractor must provide ongoing technical support/ maintenance throughout the	Professional Services	As necessary

	term of the contract.		
Completion of Project Stages/ Project Closure	The contractor must participate in meetings and provide pertinent support/ technical assistance and guidance as related to each stage of the project.	Professional Services	As necessary
Reporting	The contractor must provide a status report for each deliverable in Table 2.1.4. Deliverables of NNS.	Documents (including, but not limited to, bi-weekly status/ progress reports)	As necessary

## 2.2. Technical, Operational and Organizational Environment

Table 2.2.1. Technical Scalability Requirements (TS) of NNS

Reference #	Technical Scalability Requirements	Priority
TS-001	System must enable up to 100 Business Administrators, Schedulers and Travel Teams to concurrently add and/ or edit data without performance degradation.	Must Have
TS-002	System must enable up to 3000 HCPs to be concurrently logged in and viewing their schedules (read-only ability) without performance degradation.	Must Have

## 2.3. Method and Source of Acceptance

Payment of the fees will be made upon the contractor's completion of tasks as evidenced by the completion of the specified deliverables. Payments will be made only after receipt of such Deliverables and acceptance.

The final work will be accepted when the contractor has completed all of the requirements indicated in the Statement of Work; Canada has reviewed the documents and asked for changes if needed and the ISC Authority has signed off and approved the system and accompanying documentation as being completed and accurate based on the requirements set forth by ISC.

Except as otherwise specifically provided for herein, ISC will not be required to pay for partially completed tasks or for any additional Work that may be required that the contractor has not budgeted for in its proposal.

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 Authority before their incorporation into the Work.

## 2.4. Data Hosting and Ownership Requirements

- Designated ISC employees shall have access to all back-end data at all times, including during system outages and other maintenance;
- The contractor is required to provide “READ Access” and privileges to the ISC DBA team to perform the required data extraction and/ or duplication from the system database into the (ISC) departmental infrastructure premises;
- System shall enable Power-BI integration for more advanced analytics and data visualizations, and;
- ISC owns all its data.

## 3. ADDITIONAL INFORMATION

### 3.1. Authorities

Table 3.1.1. Authorities of NNS

Roles	Titles
Project Sponsor	Senior Director, Primary Health Care Services & Deputy Chief Nursing Officer
Project Lead	Project Manager / Senior Program Officer, Centre for Nursing Workforce
Project Lead	Senior Program Officer, Centre for Nursing Workforce
CRM Support	Client Relations Manager, Information Management Branch
Business Planning Support	Senior Program Officer, Internal Client Services
IT Support	Consultant, Cyber Security/IT Security and Business Continuity Planning
IM Support	Information Management Officer, Enterprise IM
Procurement Support	Senior Procurement Officer, Procurement Operations

### 3.2. Contractor’s Obligations

Unless otherwise specified, the contractor must use its own equipment and software for the performance of this Statement of Work.

### 3.3. Location of Work

The Work must be carried out on the premises of the contractor.

### 3.4. Language of Work

NNS must be available and fully functional in both of Canada's official languages (English and French). In addition, all required documentation and support (written and verbal) must be available and provided in English and French.

### 3.5. Insurance Requirements

The contractor must obtain and maintain an appropriate level of professional liability insurance coverage.

### 3.6. Travel and Living

Payment for travel and living expenses must be made in accordance to the terms of payment and the National Joint Council Travel Directive.

## 4. PROJECT SCHEDULE

### 4.1. Expected Start and Completion Dates

The services of the contractor will be required for a period of approximately (six years) commencing on or about (01 April 2024).

### 4.2. Schedule

Table 4.2.1. Schedule of NNS

Activity	Date
Configuration	Date(s) to be determined 10 business days after project kick-off meeting
Security Deliverables, Authority to Operate	
Testing	
Train Users	
Go live	
Implementation Close-Out	

## 5. REQUIRED RESOURCES OR TYPES OF ROLES TO BE PERFORMED

The contractor must provide a Project Manager or Account Representative to support the delivery of Work as per the Statement of Work.

## 6. APPLICABLE DOCUMENTS AND GLOSSARY

### 6.1. Applicable Documents

The relevant links in Annex A – Statement of Work have been provided as references. The links were valid at the time of initial publication of this document; however, they may change or cease to work throughout the duration of the contract.

### 6.2. Glossary of Terminology

Table 6.2.1. Glossary of Terminology of NNS



<b>Term</b>	<b>Definition</b>
Business Administrators:	means a User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements.
Contract Health Care Professionals:	means a non-Indigenous Services Canada employed Registered Nurse, Nurse Practitioner, Licensed Practical Nurse, Registered Practical Nurse, Primary Care Paramedic, Advanced Care Paramedic, Critical Care Paramedic, and/ or other designations of professional providing health-related services to Indigenous Peoples.
Data Team:	means a User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements.
Health Care Professionals:	means a Registered Nurse, Nurse Practitioner, Licensed Practical Nurse, Registered Practical Nurse, Primary Care Paramedic, Advanced Care Paramedic, Critical Care Paramedic, and/ or other designations of professional providing health-related services to Indigenous Peoples, and whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements.
Health Facilities:	means a health care facility within which primary care and public health services are delivered (e.g., nursing station, health centre, with or without treatment, hospital).
Nurse In Charge (NIC):	means a User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements.
Nurse Management:	means a User of NNS who is an (Acting) Nurse Manager and whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements.
Schedulers:	means a User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements.
Travel Team:	means a User of NNS whose functionality is outlined in section 2. Requirements, Table 2.1.2. Functional Requirements.
User(s):	means a person and/ or group who uses NNS.  All Users of NNS will create, collect, receive, manage, access, use, retain and dispose of personal information only for the purposes relating to their duties, and do so in accordance with the Privacy Act and TBS privacy and security policies and directives.

### 6.3. Glossary of Acronyms

Table 6.3.1. Glossary of Acronyms of NNS

<b>Acronym</b>	<b>Meaning</b>
FN	First Nations
FNHIB	First Nations and Inuit Health Branch
HCP	Health Care Professional
ISC	Indigenous Services Canada

LPN	Licensed Practical Nurse
NIC	Nurse In Charge
NM	Nurse Management
NNS	National Nurse Scheduler
NP	Nurse Practitioner
NRCU	Nursing Relief Coordination Unit
RN	Registered Nurse
RPN	Registered Practical Nurse

## 7. APPENDICES

Annex B\_to SoW Schedule 1\_Security Obligations \* Attached separately

Annex B\_to SoW Schedule 2\_Privacy Obligations \* Attached separately

## Cloud Security Obligations for Cloud SAAS provider – PA/M/M – National Nurse Scheduler

### 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 Canada'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**").

#### 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 as set forth in this Schedule.

The Contractor must advise Canada of all changes that materially degrades or may have an adverse affect 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 Canada.

### 2. Acknowledgments

The parties acknowledge that:

- (a) Canada'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 Canada's Data.
- (c) The Contractor must not have or attempt to gain custody of Canada's Data, nor permit any Cloud Services Personnel to access Canada's Data prior to the implementation of the Security Requirements as required under this Schedule on or before Contract Award.
- (d) Security Obligations apply to **Commercial Cloud Services** (up to and including Protected A / Medium Integrity, Medium Availability or Medium Injury), unless otherwise specified.

### 3. Securing Canada's Data

The Contractor must protect Canada'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 Canada'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 Canada. 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 Canada 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 Canada.

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

(1) The Contractor must ensure that Canada's Data, Contractor Infrastructure (including any IaaS, PaaS or SaaS Service provided to Canada) 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 independent third-party assessment reports or certifications 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 subsequent versions); AND

(b) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services achieved by an accredited certification body (or subsequent versions); AND

(c) 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.

(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 Canada. 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 and provide Canada with supporting evidence of the remediation measures taken or confirmation from the auditor that issues have been remediated 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 its certification of ISO 27001, ISO 27017, and/or SOC 2 Type II as applicable for the duration of the contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

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

(1) In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with Section 5 - Third-Party Assurance and has already been assessed by Canadian Centre for Cyber Security (CCCS) under the CSP ITS Assessment Program, the SaaS provider must provide Canada with a copy of an email provided by the Canadian Centre for Cyber Security (CCCS) confirming that the Bidder has completed the CCCS CSP ITS Assessment Program. The email must state that the CSP has been assessed by the CSP ITS Assessment Program and that the CSP has received a

final report with regards to the assessment. For any questions, CCCS can be contacted by email at [contact@cyber.gc.ca](mailto:contact@cyber.gc.ca).

(2) In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider but this Contractor has not already been assessed by Canadian Centre for Cyber Security (CCCS) under the CSP ITS Assessment Program, the Contractor must be available to undergo an assessment of its offering in the goal of demonstrating its compliance with the security requirements selected in the "Canadian Centre for Cyber Security (CCCS) Annex A Cloud Control Profile – Low", of the Guidance on Security Categorization of Cloud-Based Services (ITSP.50.103) (<https://www.cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103>) for the scope of the Cloud Services provided by the Contractor. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified above (para 5), and validated through independent third-party assessments.

(3) Compliance will be assessed and validated through the CCCS CSP Information Technology (IT) Security Assessment Process (ITSM.50.100) (<https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100>).

### **7. Industrial Security Program – Security Requirement for Canadian Suppliers**

(1) The Contractor/Offeror 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 Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC)

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

(3) 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 including an IT Link at the level of PROTECTED A.

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

(5) The Contractor/Offeror must comply with the provisions of the: (a) Security Requirements Check List and security guide (if applicable), attached at Annex B and C;

**ANNEX "B"**

**BASIS OF PAYMENT**

The Contractor will be reimbursed for the costs reasonably and properly incurred in the performance of the work as determined in Annex – “A” – Statement of Work; to a limitation of expenditure of \$\_\_\_\_\_.

<b>CONTRACT PERIOD: Contract period is 4 years from contract award.</b>				
<b>(A)</b>	<b>(B)</b>	<b>(C)</b>		<b>(D)</b>
	<b>1,750 Licenses</b>	<b>Optional licenses (price for additional 250)</b>	<b>Professional Fees (including vendor’s scheduling software/ system, and all other applicable costs to deliver work as per the SOW)</b>	<b>Total Cost</b>
<b>Year 1</b>	\$	\$	\$	\$
<b>Year 2</b>	\$	\$	\$	\$
<b>Year 3</b>	\$	\$	\$	\$
<b>Year 4</b>	\$	\$	\$	\$
<b>Total Estimated Initial Contract Cost:</b>				\$
<b>Applicable Taxes to Professional Fees</b>				\$
<b>GRAND TOTAL</b>				\$

<b>Option Period 1</b>				
<b>(A)</b>	<b>(B)</b>	<b>(C)</b>		<b>(D)</b>
	<b>1,750 Licenses</b>	<b>Optional licenses (price for additional 250)</b>	<b>Professional Fees (including vendor’s scheduling software/ system, and all other applicable costs to deliver work as per the SOW)</b>	<b>Total Cost</b>

<b>Year 5</b>	\$	\$	\$	\$
<b>Total Estimated Initial Contract Cost:</b>				\$
<b>Applicable Taxes to Professional Fees</b>				\$
<b>GRAND TOTAL</b>				\$

<b>Option Period 2</b>				
(A)	(B)	(C)		(D)
	<b>1,750 Licenses</b>	Optional licenses (price for additional 250)	Professional Fees (including vendor's scheduling software/ system, and all other applicable costs to deliver work as per the SOW)	<b>Total Cost</b>
<b>Year 6</b>	\$	\$	\$	\$
<b>Total Estimated Initial Contract Cost:</b>				\$
<b>Applicable Taxes to Professional Fees</b>				\$
<b>GRAND TOTAL</b>				\$

## ANNEX "C"

## SECURITY REQUIREMENTS CHECK LIST


 Contract Number / Numéro du contrat  
 1000254069/

 Security Classification / Classification de sécurité  
 Unclassified

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

PART A – CONTRACT INFORMATION / PARTIE A – INFORMATION CONTRACTUELLE	
1. Branch / Sector / Directorate / Region / Direction générale / Secteur / Direction / Région ISC-FNIHB-PHPCD-OPHC-CNW - NCR	2. Contract type / Type de contrat Non-Competitive / Non-compétitif <input type="checkbox"/> Competitive / Compétitif <input checked="" type="checkbox"/> Type : RFP
3. Brief Description of Work / Brève description du travail In order for FNIHB to achieve its mandate, as well deliver high-quality healthcare, a centralized nurse scheduling solution is imperative. This enables FNIHB to ensure that nurses and paramedics, with the required qualifications, are scheduled (and present) in the nursing stations and health centres when needed. In addition, a National Nurse Scheduler (NNS) allows FNIHB to analyse staffing situations and trends, and, with that information, make informed decisions related to staffing requirements in the Indigenous communities we serve. Our current (sole source) contract for "FNIHB Nurse Scheduling" expires June 30, 2024.	
4. Contract Amount / Montant du contrat \$1,020,000. - \$170,000. per year - 4 years + 2 one year option periods	6. Company Name and Address (for non-competitive contract only) / Nom et adresse de la compagnie (pour les contrats non-compétitifs seulement) : To Be Determined
5. Contract Start and End date / Date de début et de fin du contrat April 1, 2024 – March 31, 2030	
7. Will the supplier require / Le fournisseur aura-t-il :	
7.1 access to PROTECTED and/or CLASSIFIED information or assets? accès à des renseignements ou à des biens désignés PROTÉGÉS et/ou CLASSIFIÉS?	<input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui
7.2 an access card to AANDC premises? besoin d'une carte d'accès aux bureaux d'AANDNC?	<input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui
7.3 access to the departmental computer network? accès au réseau informatique du Ministère?	<input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui
<b>(If the answer is No to all three questions, go to Part D / Si la réponse est Non aux trois questions, allez à la Partie D)</b>	
PART B – SAFEGUARDS OFF-SITE (COMPANY) / PARTIE B – MESURES DE PROTECTION À L'EXTÉRIEUR (COMPAGNIE)	
PHYSICAL INFORMATION / ASSETS / RENSEIGNEMENTS MATÉRIELS / BIENS	
8. Will the supplier be required to receive/store PROTECTED and/or CLASSIFIED information/assets on its site or premises? Le fournisseur sera-t-il tenu de recevoir /entreposer sur place des renseignements/biens PROTÉGÉS et/ou CLASSIFIÉS? <input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui	
INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)	
9.1 Will the supplier be required to use its computers, portable media, or IT systems to electronically process/store sensitive information? Le fournisseur sera-t-il tenu d'utiliser ses propres ordinateurs, médias portatifs ou systèmes TI pour traiter/stocker électroniquement des renseignements sensibles?	<input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui
9.2 Will the supplier be required to electronically transmit sensitive information to/from the Department or with other parties? Le fournisseur sera-t-il requis de transmettre électroniquement de l'information sensible au/à partir du Ministère ou avec d'autres parties? If yes, specify: / Si oui, spécifiez :	<input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui
a) Email transmission / Transmission par courrier électronique :	<input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui
b) Other transmission (Secure FTP, Collaboration, etc) / Autre transmission (FTP sécurisé, collaboration, etc) :	<input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui
c) Remote access required to AANDC network (VPN, Citrix) / Besoin de connexion à distance au réseau d'AANDNC (VPN, Citrix) :	



9.3 Will the supplier be required to safeguard COMSEC\* information or assets?

Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC\* ?

No  
 Non  
 Yes  
 Oui

\* Handling equipment and measures for secure transmission and emission (cryptographic, secure fax/phone)/ Manipulation de l'équipement et des mesures sécuritaires pour fin de transmission et émissions (cryptographie, téléphone/télécopieur sécuritaire)

#### 10. SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	Please refer to question ; Veuillez vous référer à la question :	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ		
		A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET
Information /Assets Renseignements/Biens	7.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information /Assets (off site) Renseignements/Biens (extérieur)	8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IT Information /Assets (off site) Renseignements/Biens TI (extérieur)	9.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IT Transmission – e-mail Transmission TI - courriel	9.2 a)	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
IT Transmission – other Transmission TI - autre	9.2 b)	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Remote Access to Network Connexion à distance au réseau	9.2 c)	<input type="checkbox"/>	<input type="checkbox"/>				
COMSEC	9.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### PART C – PERSONNEL / PARTIE C – PERSONNEL

11.1 Personnel Security Screening Level Required:

Niveau d'enquête de la sécurité du personnel requis :

N/A /  
Non requis  Reliability/  
Fiabilité  Confidential/  
Confidentiel  Secret  Top Secret/  
Très secret

11.2 May unscreened personnel be used for portions of work?

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

No  
Non  Yes  
Oui  N/A /  
Non requis

12. 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



Contract Number / Numéro du contrat  
**1000254069/**  
 Security Classification / Classification de sécurité  
 Unclassified

PART D – AUTHORIZATION / PARTIE D – AUTORISATION			
13. Organization Project Authority / Chargé de projet de l'organisme Name (print) – Nom (en lettres moulées) Janice Tario		Title - Titre Manager – Centre for Nursing Workforce (CNW)	Signature <b>tario, janice</b> <small>Digitally signed by tario, janice Date: 2023.08.21 10:50:26 -04'00'</small>
Telephone No. – N° de téléphone (613) 222-5559	Facsimile No. - N° de télécopieur n/a	E-mail address – Adresse courriel janice.tario@sac-isc.gc.ca	Date 2023-08-18
14. Organization Security Authority / Responsable de la sécurité de l'organisme Name (print) – Nom (en lettres moulées) Marc-André Trottier		Title - Titre Contract Security Officer	Signature <b>trottier, marcandre</b> <small>Digitally signed by trottier, marcandre Date: 2024.02.08 10:47:07 -05'00'</small>
Telephone No. – N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address – Adresse courriel marc-andre.trottier@sac-isc.gc.ca	Date
15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? <input type="checkbox"/> No / <input type="checkbox"/> Yes Non / Oui			
16. Procurement Officer / Agent d'approvisionnement Name (print) – Nom (en lettres moulées) Alex Cormier Howie		Title - Titre Senior Procurement Officer	Signature <b>cormierhowie, alex</b> <small>Digitally signed by cormierhowie, alex DN: C=CA, O=GC, OU=ISC-SAC, CN="cormierhowie, alex" Reason: I am the author of this document Location: Ottawa, Canada Date: 2023.11.08 11:50:23 -05'00" Font: PDF Editor Version: 12.1.2</small>
Telephone No. – N° de téléphone 873-354-0959	Facsimile No. - N° de télécopieur N/A	E-mail address – Adresse courriel alexander.cormierhowie@sac-isc.gc.ca	Date
17. Contracting Security Authority / Autorité contractante en matière de sécurité Name (print) – Nom (en lettres moulées) Marc-André Trottier		Title - Titre Contract Security Officer	Signature <b>trottier, marcandre</b> <small>Digitally signed by trottier, marcandre Date: 2024.02.08 10:52:48 -05'00'</small>
Telephone No. – N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address – Adresse courriel marc-andre.trottier@sac-isc.gc.ca	Date

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité  
 Unclassified



**ANNEX "D"****Security Requirements Agreement**

Company name: \_\_\_\_\_  
 Request for proposal: 1000254069  
 Contract: \_\_\_\_\_

1. **Physical Security Transportation and Safeguard Requirements**

It is important to properly safeguard sensitive information. This will assist in reducing the risk of unauthorized access, disclosure or compromise of **Sensitive** information.

1.1 **Physical Safeguards:**

The Protected documents must be safeguarded in a locked security container with access restricted to the contractor only.

	<b>Protected A</b>
<b>Container</b>	Key locked container
<b>Facility</b>	Restricted access room within office/home

**Definitions:**

**Protected information:** Information for which unauthorized disclosure, destruction, interruption, removal or modification could reasonably be expected to cause injury to an individual, organization or government which lies outside the national interest.

**Protected A:** Could cause injury. A few examples: Personal data such as names, birth dates, home address and telephone number, linguistic profiles, salary figures, Social Insurance Numbers.

1.2 **Transportation**1.2.1 **Transportation of Paper Records:**

- **Protected** documents must be securely packaged in folders carried in an approved locked briefcase.
- Sensitive information must be kept under the constant control of the contractor, including during meals and during travel.
- While on contractor premises, portable media devices containing sensitive information are equivalent to paper records and are to be physically stored within an appropriate security container such as those listed above.

1.2.2 **Prevention Tips While in Transit:**

- Prior to travel: Make an inventory of information.
- Public Areas: Sensitive information must never be read, displayed, discussed or used in public areas.
- Overnight Stopovers: Information is not to be left unattended.
- Travelling by Car: Locked in trunk while travelling. Never to be left unattended in vehicle.

- Travelling by Air: Bring with you as a carry-on.
- Hotels/Conference Centers: Be careful about sensitive conversations in hotel conference rooms.
- Never use hotel reception staff or devices to fax, receive or copy sensitive information. Ensure all participants have the proper security clearance and the need-to-know.
- In the event a device or a document is lost or stolen, it must be reported immediately to the Department.

### 1.2.3 Discussion:

- Sensitive information must never be read, displayed, discussed or used in public areas.
- Be careful about sensitive conversations in hotel conference rooms. Ensure everyone in the conference room has the proper security screening level, the need-to-know and that the door is closed.
- Do not use a wireless device to discuss sensitive matters. Use a wired telephone to discuss **Sensitive** matters.

## 2. IT Security Requirements

Production and storage of **Protected** data outside of the departmental premises must be done as per the following to ensure that the data remains secure at all times.

### 2.1 Electronic Storage

- Store **Protected** electronic documents on encrypted removable media (USB key) that use approved Government of Canada standards (FIPS 140-2 or above (ex: FIPS 140-3) certified removable media device, encrypted with AES 128, 192 or 256 bit algorithm and not be copied to a device which does not meet these requirements.  
<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm>)
- Select strong passwords for your encrypted USB keys. The level of protection provided by such devices is directly related to the strength of the password chosen.

### 2.2 Electronic Possession, Transportation and Processing

When there is a requirement for the contractor to transport, process or electronically store departmental information, the contractor must ensure that the data remains secure at all times no matter what level of confidentiality the information is by adhering to the following requirements:

- Computing devices used to process data are equipped with up to date anti-virus software which is configured to automatically receive and install product updates;
- Computing devices used to process data must be equipped with up to date software and Operating System versions, and configured to automatically receive and install updates;
- Computing devices are protected by a firewall which can be a network perimeter firewall appliance or host based firewall application installed on the computer (note: a standard router only device is not considered a substitute to a firewall);
- The contractor has the means to securely dispose of electronic data in accordance with CSEC standards (refer to <https://cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006>  
Departmental data must be stored on a FIPS 140-2 or above certified removable media device that is encrypted with AES 128 bit algorithm or higher (refer to <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm> for a list of certified devices); and
- Portable storage devices must be labeled to indicate the highest classification or designation level of information stored on the device.

### 2.3 Electronic Transmission of Departmental Data

Electronic transmission of Protected data between the Contractor and the Department of Crown-Indigenous Relations and Northern Affairs Canada (CIRNAC) and Indigenous Services Canada (ISC) must be done as per the following approved method based on the level of sensitivity of the information. The contractor may use a combination of these transmission methods in order to share information with CIRNAC/ISC's personnel. The use of electronic transmission methods other than those listed below is prohibited.

Classification Level	CIRNAC/ISC Approved Transmission Methods	Requirements
<b>Protected A</b>	Email	<p>The Contractor can transmit Protected A Data to CIRNAC/ISC personnel via email as long as the following requirements are met:</p> <ul style="list-style-type: none"> <li>• The e-mail account is not a publically accessible web-mail based service (ex: hotmail, yahoo mail, gmail etc);</li> <li>• Each user has their own corporate e-mail account which is protected with a username and password; and</li> <li>• Email server communication is protected with TLS encryption.</li> </ul>
	Fax	<p>The Contractor can transmit Protected A Data to CIRNAC/ISC via fax as long as the following requirements are met:</p> <ul style="list-style-type: none"> <li>• The sending fax machine is located on the contractor's premises;</li> <li>• The sender contacts the recipient to confirm fax number and advise recipient of incoming fax;</li> <li>• Recipient is present at the fax machine ready to receive fax; and</li> <li>• Sender obtains confirmation from sender of receipt.</li> </ul>
	Wireless Communications	<p>If a wireless access point is installed on the contractor's premises, and devices processing CIRNAC/ISC data will be connected to this network, the wireless infrastructure must at a minimum include the following safeguards:</p> <ul style="list-style-type: none"> <li>▪ The administrator user name and password must be changed from their default values;</li> <li>▪ The network name (SSID) has been changed from its default value; and</li> <li>▪ WPA2 encryption with an AES algorithm enabled and the passphrase meets the following complexity requirements: <ul style="list-style-type: none"> <li>• Must be 8 characters or longer;</li> <li>• Have at least one upper case character;</li> <li>• Have at least one lower case character;</li> </ul> </li> </ul>

		<ul style="list-style-type: none"><li>• Have at least one numeric character; and</li><li>• Have at least one allowed special character</li></ul>
--	--	--

3. Inspection

An authorized representative of the Government shall have the right to inspect, at reasonable intervals, the Contractor's methods and facilities for compliance with the Policy on Government Security requirements and this Agreement. The Contractor shall cooperate with the authorized representative and provide such information as the authorized representative may require in regard to any such inspections. Should the Government determine that the Contractor is not in compliance, it shall submit a written report to the Contractor advising of the deficiencies and follow-up on the deficiencies until they are rectified to the satisfaction of the department.

4. Security Costs

The Department shall not be liable for any costs or claims of the Contractor arising out of this Agreement or instructions issued hereunder.

## SECURITY AGREEMENT

I, \_\_\_\_\_ (Contractor) and authorized resources will fulfill the duties as contractor working under the contract \_\_\_\_\_, as set out below, to the best of our abilities.

1. Will abide by all of Indigenous Services Canada (ISC) security clauses and requirements included in this contract. Acknowledge receipt and understand these existing clauses and requirements, and promise to familiarize with any amendments to them, forthwith after receipt of such amendments.
2. Understand and agree that information received in the process of performing our duties in relation to this contract is subject to the Policy on Government Security and may be also subject to the Privacy Act, and will remain the property of CIRNAC/ISC. Without the prior written authorization of CIRNAC/ISC or of the person to whom the information relates, this information can only be viewed by myself and authorized resources and may only be used for the purposes of this contract on behalf of CIRNAC/ISC.
3. Agree to notify ISC authorities of any unauthorized access, disclosure or misuse of the sensitive information of which we become aware and will provide full details of the incident immediately noting the corrective action taken to prevent a recurrence of the incident.
4. Understand and agree that any additional resources authorized to perform work under this contract will also abide by all of ISC security clauses and requirements included in this contract.