	Canada Revenue Agency	Agence du revenu du Canada

RETURN BIDS TO :
RETOURNER LES SOUMISSION À:

Canada Revenue Agency
Agence du revenu du Canada

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

Proposition à : l'Agence du revenu du Canada
Nous offrons par la présente de vendre à Sa Majesté la Reine du Chef du Canada, en conformité avec les conditions énoncées dans la présente incluses par référence dans la présente et/ou incluses par référence aux annexes jointes à la présente les biens et/ou services énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Bidder's Legal Name and Address (ensure the Bidder's complete legal name is properly set out)
Raison sociale et adresse du Soumissionnaire (s'assurer que le nom légal au complet du soumissionnaire est correctement indiqué)

_____

_____

_____

Bidder MUST identify below the name and title of the individual authorized to sign on behalf of the Bidder – Soumissionnaire doit identifier ci-bas le nom et le titre de la personne autorisée à signer au nom du soumissionnaire

_____

Name /Nom

_____

Title/Titre

_____

Signature

_____

Date (yyyy-mm-dd)/(aaaa-mm-jj)
(____)_____
Telephone No. – No de téléphone
(____)_____
Fax No. – No de télécopieur

_____

E-mail address – Adresse de courriel

REQUEST FOR PROPOSAL /
DEMANDE DE PROPOSITION

Title – Sujet
Emergency Mass Notification Software Solution (EMNSS)

Solicitation No. – No de l'invitation	**Date**
1000348508A	**2020-02-03**

Solicitation closes – L'invitation prend fin	**Time zone – Fuseau horaire**
on – le 2020-03-16 at – à 2:00 P.M. / 14 h	EDT Eastern Daylight Time

Contracting Authority – Autorité contractante

Name – Alastair Webb

E-mail address - alastair.webb@cra-arc.gc.ca

Telephone No. – No de téléphone
(613) 867-5203

Destination - Destination

See herein / Voir dans ce document

PART 1: GENERAL INFORMATION

1.1 Introduction

The solicitation is divided into seven parts plus appendices and annexes, as follows:

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

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

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

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

Part 5   Certifications and Additional Information: includes the certifications to be submitted with the bid and before contract award;

Part 6   Security Requirements; and

Appendices

Appendix 1: Mandatory Criteria
Appendix 2: Financial Bid

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

Annexes to the resulting contract

Annex A: STATEMENT OF REQUIREMENT (SOR)
Annex B: BASIS OF PAYMENT
Annex C: SECURITY REQUIREMENTS CHECKLIST (SRCL)

1.2 Summary

Background
The Canada Revenue Agency (CRA) has approximately 47000 employees in 99 buildings across the country and as such there is a requirement to effectively communicate with employees before, during and after an emergency event. The Security and Internal Affairs Directorate, Finance and Administration Branch has identified the need to acquire an Emergency Mass Notification Software Solution (EMNSS) that will allow for a more efficient and consistent method of communicating with CRA employees before, during and after an emergency event.

The CRA has a requirement for the supply of an EMNSS that will deliver, allow and support the broadcast notifications of threats or emergency events. The EMNSS provided by the Contractor must be able to send out mass notifications to all CRA employees. The EMNSS will be used within CRA as a notification instrument for their own employees and students.

1.3   Debriefings

Bidders may request a debriefing on the results of the solicitation process. Bidders should make the request to the Contracting Authority within ten (10) business days of receipt of the results of the solicitation process. The debriefing may be in writing, by telephone or in person.

1.4   Office of the Procurement Ombudsman (OPO)

The Office of the Procurement Ombudsman (OPO) was established by the Government of Canada to provide an independent avenue for suppliers to raise complaints regarding the award of contracts under $25,000 for goods and under $100,000 for services. If you have issues or concerns regarding the solicitation, you have the option of raising them with the CRA, or, you may have the option of raising them with the OPO depending upon the nature of the complaint.   You may contact the OPO by telephone at 1-866-734-5169 or by e-mail at boa.opo@boa.opo.gc.ca. You can also obtain more information on the OPO services available to you at their website at www.opo-boa.gc.ca .

1.5   Canadian International Trade Tribunal

As a general rule, a complaint regarding this procurement process must be filed with the Canadian International Trade Tribunal (the Tribunal) within 10 working days from the date on which a bidder becomes aware, or reasonably should have become aware, of a ground of complaint. Alternatively, within that time frame, a bidder may first choose to raise its ground of complaint by way of an objection to the CRA; if the CRA denies the relief being sought, a bidder may then file a complaint with the Tribunal within 10 working days of that denial. More information can be obtained on the Tribunal's Web site (www.citt-tcce.gc.ca) or by contacting the Registrar of the Tribunal at 613-993-3595.

Also consult Recourse Mechanisms (https://buyandsell.gc.ca/for-businesses/selling-to-the-government-of-canada/recourse-mechanisms).

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 issued by Public Services and Procurement Canada (PSPC). The Manual is available on the PSPC Website: https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual.

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

The standard instructions and conditions 2003 (2016-04-04) are incorporated by reference into and form part of the bid solicitation.

2.1.1   Revisions to Standard Instructions 2003

Standard Instructions - Goods or Services – Competitive Requirements 2003 (2016-04-04) are revised as follows.

Section 01 titled "Integrity Provisions– Bid", is deleted in its entirety and replaced with the following :

1. The *Supplier Integrity Directive* (SID) dated May 24, 2016, is incorporated by reference into, and forms a binding part of the bid solicitation. The Bidder must comply with the SID, which can be found on the Canada Revenue Agency's website at *https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/procurement-cra/supplier-integrity-directive.html*.

2. Under the SID, charges and convictions of certain offences against a Supplier, its affiliates or first tier subcontractors, and other circumstances, will or may result in a determination by Public Works and Government Services Canada (PWGSC) that the Supplier is ineligible to enter, or is suspended from entering into a contract with Canada. The list of ineligible and suspended Suppliers is contained in PWGSC's Integrity Database. The SID describes how enquiries can be made regarding the ineligibility or suspension of Suppliers.

3. In addition to all other information required in the bid solicitation, the Bidder must provide the following:

    a. by the time stated in the SID, all information required by the SID described under the heading "Mandatory Provision of Information"; and

    b. with its bid, a complete list of all foreign criminal charges and convictions pertaining to itself, its affiliates and its proposed first tier subcontractors that, to the best of its knowledge and belief, may be similar to one of the listed offences in the SID. The list of foreign criminal charges and convictions must be submitted using an Integrity Declaration Form, which can be found at Declaration form for procurement.

4. Subject to subsection 5, by submitting a bid in response to this bid solicitation, the Bidder certifies that:

    a. it has read and understands the SID (https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/procurement-cra/supplier-integrity-directive.html)

    b. it understands that certain domestic and foreign criminal charges and convictions, and other circumstances, as described in the SID, will or may result in a determination of ineligibility or suspension under the SID;

    c. it is aware that Canada may request additional information, certifications, and validations from the Bidder or a third party for purposes of making a determination of ineligibility or suspension;

    d. it has provided with its bid a complete list of all foreign criminal charges and convictions pertaining to itself, its affiliates and its proposed first tier subcontractors that, to the best of its knowledge and belief, may be similar to one of the listed offences in the SID;

e. none of the domestic criminal offences, and other circumstances, described in the SID that will or may result in a determination of ineligibility or suspension, apply to it, its affiliates and its proposed first tier subcontractors; and

f. it is not aware of a determination of ineligibility or suspension issued by PWGSC that applies to it.

5. Where a Bidder is unable to provide any of the certifications required by subsection 4, it must submit with its bid a completed Integrity Declaration Form, which can be found at Declaration form for procurement.

6. Canada will declare non-responsive any bid in respect of which the information requested is incomplete or inaccurate, or in respect of which the information contained in a certification or declaration is found by Canada to be false or misleading in any respect. If Canada establishes after award of the Contract that the Bidder provided a false or misleading certification or declaration, Canada may terminate the Contract for default. Pursuant to the SID, Canada may also determine the Bidder to be ineligible for award of a contract for providing a false or misleading certification or declaration.

Section 02 titled "Procurement Business Number", is hereby deleted in its entirety and replaced with: Suppliers should obtain a Business Number (BN) before contract award. Suppliers may register for a BN online at http://www.cra-arc.gc.ca/tx/bsnss/tpcs/bn-ne/menu-eng.html.

Section 03 titled "Standard Instructions, Clauses and Conditions", "Pursuant to the Department of Public Works and Government Services Act (S.C. 1996, c.16)," is hereby deleted.

Section 05 titled "Submission of Bids", paragraph 2 (d) is deleted in its entirety and replaced with the following: (d) send its bid only to the Canada Revenue Agency Bid Receiving Unit or to the address specified in the solicitation in Section 2.3.

Section 05 titled "Submission of Bids" paragraph 4, delete 60 days and replace with 180 days.

Section 06 titled "Late Bids" reference to "PWGSC" is hereby deleted and replaced with CRA.

Section 07 titled "Delayed Bids" all references to "PWGSC" are hereby deleted and replaced with "CRA".

Section 12 titled "Rejection of Bid", delete subsections 1(a) and 1(b) in their entirety.

Section 20 titled "Further Information", Paragraph 2 is hereby deleted and replaced with the following: Enquiries concerning receipt of bids may be addressed to the Contracting Authority identified in the bid solicitation.

Section 21 titled "Code of Conduct for Procurement-bid" is hereby deleted in its entirety.

2.2   Terms and Conditions

The Bidder hereby certifies compliance with and acceptance of all of the articles, clauses, terms and conditions contained or referenced in this Request for Proposal (RFP) and Statement of Requirement (SOR). Any modifications or conditional pricing by the bidder, including deletions or additions to the articles, clauses, terms and conditions contained or referenced in this RFP and/or SOR document will render the bid non-responsive and the bid will receive no further consideration.

2.3   Enquiries - Solicitation Period

All enquiries must be submitted to the Contracting Authority no later than five 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.

2.4 Applicable Laws

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

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

2.5 Submission of Bids

Bids must be delivered only to the CRA Bid Receiving Unit indicated below by the time and date indicated on Page 1 of the bid solicitation.

BIDDERS ARE TO SUBMIT BIDS TO:
Canada Revenue Agency
Bid Receiving Unit
Ottawa Technology Centre
Receiving Dock
875 Heron Road, Room D-95
Ottawa, ON K1A 1A2
Telephone No: (613) 941-1618

Bidders are hereby advised that the Bid Receiving Unit of CRA is open Monday to Friday inclusive, between the hours of 0730 and 1530, excluding those days that the federal government observes as a holiday.
ELECTRONIC BIDS WILL NOT BE ACCEPTED. Due to the nature of this solicitation, electronic transmissions of a bid by such means as electronic mail or facsimile is not considered to be practical and therefore will not be accepted.

PART 3:   BID PREPARATION INSTRUCTIONS

3.1   Bid – Number of Copies

Canada requests that bidders provide their bid in separately bound sections as follows:

<u>Section I</u>:   Technical Bid (4 hard copies, and 1 soft copy on USB)

<u>Section II</u>:   Financial Bid (1 hard copy, and 1 soft copy on USB)

<u>Section III</u>:   Certifications (1 hard copy and 1 soft copy on USB)

Bidders must submit the certifications required under Part 5.

<u>Section IV</u>:   Additional Information (1 hard copy, and 1 soft copy on USB)

If there is a discrepancy between the wording of the soft copy and the hard copy, the wording of the hard copy will have priority over the wording of the soft copy.

3.2   Bid Format and Numbering System

Canada requests that bidders follow the format instructions described below in the preparation of their bid.

a. use 8.5 x 11 inch (216 mm x 279 mm) paper;
b. Use recycled-fibre content paper and two-sided printing. Reduction in the size of documents will contribute to CRA's sustainable development initiatives and reduce waste;
c. avoid the use of colour and glossy formats
d. use a numbering system corresponding to that of the bid solicitation;
e. include the certification as a separate section of the bid.

3.3   Section I: Technical Bid

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

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

3.4   Section II: Financial Bid

Bidders must submit their financial bid in accordance with the format outlined in Appendix 2: Financial Proposal. The total amount of Applicable Taxes must be shown separately.

Prices must appear in the financial proposal only. No prices must be indicated in any other section of the bid. Prices are exclusive of tax.

Bidders must provide a price, percentage, or weight, as applicable, for each item identified in the format specified in Appendix 2: Financial Proposal. Ranges (e.g., $10-$13) are not acceptable.

Should the Bidder not provide a price, percentage, or weight (for example: the space is left blank or struck through or the letters N/A or the words "no charge" or "included") for one or more items in Appendix 2: Financial Proposal the following steps will be taken:

    i.   The CRA Contracting Authority will notify the Bidder of any omission(s) in its financial proposal and give it the opportunity to withdraw its bid, or agree to the following process:

    ii.   If the Bidder does not wish to withdraw its bid, CRA will insert a price of $0.00 for evaluation purposes for all cells in which financial information is omitted. The price of $0.00 would also be reflected in any resulting contract and the Bidder would be obliged to honour those prices for the period of the contract, including any option period, as applicable.

    iii.   The Bidder must advise the Contracting Authority of its decision to withdraw the bid or agree to the process described above in writing, within two (2) business days of notification. If the Bidder does not respond within the two (2) business days, CRA will render the bid non-responsive and the bid will receive no further consideration.

3.4.1   Exchange Rate Fluctuation

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

3.5   Section III: Certifications

Bidders must submit the certifications required under Part 5.

3.6   Section IV: Additional Information

Bidders must submit additional information required under Part 5.

PART 4:   **EVALUATION AND SELECTION**

4.1   Evaluation Procedures

4.1.1   Bids will be assessed in accordance with the entire requirement of the bid solicitation including the evaluation criteria. There are several steps in the evaluation process which are described below.

4.1.2   A committee composed of representatives of CRA will evaluate the bids on behalf of the Agency. The services of independent consultants may be called upon to assist in the evaluation of, or in the validation of, specific aspects of the solution proposed. CRA reserves the right to engage any independent consultant, or use any Government resources, which it deems necessary to evaluate any bid.

4.1.3   Bidders are advised that only listing experience without providing any supporting information to describe where and how such experience was obtained will not be considered to be demonstrated for the purpose of the evaluation. The Bidder should not assume that the evaluation team is necessarily cognizant of or knowledgeable about the experience and capabilities of the Bidder or any of the proposed resource(s); as such, any relevant experience must be demonstrated in the Bidders' written bid.

4.1.4   In addition to other time periods established in the bid solicitation:

   a. **Requests for Clarification:** Should the CRA seek clarification or verification from the Bidder about its bid, the Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to the CRA. Failure to meet this deadline will result in the bid being declared non-responsive.

   b. **Requests for further information:** If the CRA requires additional information pursuant to the Section entitled "Conduct of Evaluation" in 2003, Standard Instructions – Goods or Services – Competitive Requirements, to verify any or all information provided by the Bidder in its bid, the Bidder must provide the information requested within 2 working days (or a longer period if specified in writing by the Contracting Authority) of a request by the Contracting Authority.

   c. **Extension of Time:** If additional time is required by the Bidder, the Contracting Authority may grant an extension at his or her sole discretion.

4.2   Steps in the Evaluation Process

   The selection process to determine the successful Bidder will be carried out as follows:

   Notwithstanding Step 1 below, in order to expedite the evaluation process, CRA reserves the right to conduct Step 2 - Evaluation of Financial Proposals concurrently with Step 1. Should CRA elect to conduct Step 2 prior to the completion of Step 1, the information in the Financial Proposal will not be disclosed to the team evaluating the mandatory section until the completion of Step 1. However, if the Contracting Authority is able to ascertain that a proposal is non-responsive by virtue of incomplete information or an error in the financial proposal, the Contracting Authority will advise the team evaluating the mandatory section that the proposal is not compliant and should no longer be considered. The concurrent evaluation of the financial proposal does not in any way construe compliance in Step 1 despite the statement "All bids meeting the minimum thresholds in Step 1 will proceed to Step 2".

   Bids will be ranked in accordance with the Selection Methodology.

   Step 1 – Evaluation against Mandatory Criteria

   All bids will be evaluated to determine if the mandatory requirements detailed in Appendix 1 "Mandatory Criteria" have been met. Bids that do not comply with every mandatory requirement will be declared non-responsive. Only those bids meeting all mandatory requirements will then be evaluated in accordance with Step 2 below.

Step 2 – Evaluation of Financial Proposals

Only technically compliant bids meeting all of the requirements detailed in Step 1 will be considered at this point.

Prices submitted will be evaluated to determine the bid evaluation price as defined in Appendix 2: "Financial Proposal". Once the bid evaluation prices are determined under Step 2, the highest ranked bid will proceed to Step 3.

Step 3 – Basis of Selection

A bid must comply with the requirements of the bid solicitation and meet all mandatory technical evaluation criteria to be declared responsive. The responsive bid with the lowest evaluated price will proceed to Step 4.

Step 4 – Conditions Precedent to Contract Award

The Bidder(s) recommended for award of a Contract must meet the requirements provided in Part 5 "Certifications and Additional Information" and Part 6 "Security Requirements" of this RFP.

Step 5 – Proof of Proposal Testing

The Bidder with the highest ranked responsive bid as defined in Step 4 will proceed to the Proof of Proposal Testing phase of the evaluation; The Contracting Authority may request the Bidder to provide their proposed solution for demonstration and Proof of Proposal (POP) testing at a CRA designated site, with the participation and assistance of the Bidder.

The Contracting Authority will provide the Bidder with a listing of the mandatory and rated requirements that will be subjected to validation by the Contracting Authority a minimum of 10 calendar days before the Bidder's scheduled Proof of Proposal Testing date. We reserve the right to test any or all mandatory or point rated criteria in the RFP.

The purpose of the Proof of Proposal will be to validate the Bidder's bid and proposed solution related to the mandatory requirements. If there is an obvious discrepancy between the product or the performance of the products provided for Proof of Proposal Testing and the solution proposed in the Bidder's bid, CRA reserves the right to conduct whatever further tests are required to validate the Bidder's bid.

Within 15 business days of a request from the Contracting Authority, the Bidder with the highest ranked responsive bid must deliver their solution ready for testing on CRA equipment at a CRA designated site in the Canada National Capital Region (to be determined prior to Bidder notification). CRA will assume all costs related to the facilities provided, the required infrastructure (i.e. the CRA network) and CRA employees. All Bidder costs, including delivery of the solution and support during the POP will be the responsibility of the Bidder. CRA will conduct all tests utilizing CRA developed test procedures.

The Proof of Proposal testing timeline shall not exceed 10 business days, unless extended in writing by the Contracting Authority at CRA's sole discretion. If a deficiency is detected during the Proof of Proposal, the Bidder will have the opportunity to correct any deficiencies (including the provision of replacement equipment) during the Proof of Proposal testing, provided that all deficiencies are corrected within the 2 business days testing timeline.

If the proposed solution fails to meet one of the tested mandatory requirements of the SOR at the end of the 10 business day test period, the bid will be declared non-responsive. The Bidder will remove their solution from the test site and CRA will invite the Bidder with the next highest ranked responsive bid to participate in the Proof of Proposal testing phase of the evaluation.

CRA reserves the right to conduct POP testing after Contract award at its sole discretion.
The Bidder with the highest ranked responsive bid and having passed all of the Step 5 requirements as described above will be considered the successful Bidder for this requirement and will proceed to Step 6.

Step 6 – Contract Entry

The Bidder(s) with the highest ranked responsive bid and meeting all the requirements listed above will be recommended for award of a contract.

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. Canada will declare a bid non-responsive, or will declare a contractor in default in carrying out any of its obligations under the Contract, 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 may render the bid non-responsive or constitute a default under the Contract.

5.1   Certifications Required To Be Submitted At Time of Bid Closing

5.1.1   Joint Venture Certification *Only complete this certification if a joint venture is being proposed*

The Bidder represents and warrants the following:

(a)   The bidding entity is a contractual joint venture in accordance with the following definition. A "contractual joint venture" is an association of two or more parties who have entered into a written contract in which they have set out the terms under which they have agreed to combine their money, property, knowledge, skills, time or other resources in a joint business enterprise, sharing the profits and the losses and each having some degree of control over the enterprise.

(b)   The name of the joint venture is: _____(if applicable).

(c)   The members of the contractual joint venture are (the Bidder is to add lines to accommodate the names of all members of the joint venture, as necessary): _____

_____

(d)   The Business Numbers (BN) of each member of the contractual joint venture are as follows (the Bidder is to add lines for additional BNs, as necessary):

_____

_____

(e)   The effective date of formation of the joint venture is: _____

(f)   Each member of the joint venture has appointed and granted full authority to _____ (the "Lead Member") to act on behalf of all members as its representative for the purposes of executing documentation relating to the solicitation and any resulting contract.

(g)   The joint venture is in effect as of the date of bid submission.

This Joint Venture Certification must be signed by each member of the joint venture.

The Joint Venture Certification shall be effective throughout the entire period of the Contract, including any exercised option period, if exercised. The CRA has the right to request documentation from the Bidder evidencing the existence of the contractual joint venture.

Signature of an authorized representative of each member of the joint venture

(the Bidder is to add signatory lines as necessary):

_____	_____	_____	_____
Signature of Duly Authorized Representative	Name of Individual (Please Print)	Legal Name of Business Entity	Date
_____	_____	_____	_____
Signature of Duly Authorized Representative	Name of Individual (Please Print)	Legal Name of Business Entity	Date

5.2 Certifications Precedent to Contract Award and Associated Information

The certifications listed below should be completed and submitted with the bid but may be submitted afterwards. If any of these required certifications 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 comply with the request of the Contracting Authority and to provide the certification within the time frame provided will render the bid non responsive and the bid will receive no further consideration.

5.2.1 Authority to Grant License

The Bidder hereby warrants that either:

i. They own the intellectual property rights for all proposed software; or

ii. They have the full right and authority, granted by the owner of the software, to license all of the proposed software to CRA in accordance with the software license terms and conditions set out in this RFP.

Signature of authorized representative: _____

5.2.2 Integrity Provisions – Associated Information

By submitting a bid, the Bidder certifies that the Bidder and its Affiliates are in compliance with the provisions as stated in Section 01 Integrity Provisions - Bid of Standard Instructions 2003. The associated information required within the Integrity Provisions will assist Canada in confirming that the certifications are true.

5.2.3 Employment Equity

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

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

Canada will also have the right to terminate the Contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list during the period of the Contract.

The Bidder must provide the Contracting Authority with a completed Federal Contractors Program for Employment Equity - Certification (found below), before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

5.2.4 Vendor Reporting Information

The following information should be provided to enable CRA compliance with paragraph 221(1)(d) of the Income Tax Act, R.S.C. 1985, c.1 (5th Supp.) and report payments made to contractors under applicable services contracts (including contracts involving a mix of goods and services) on a T1204 Government Service Contract Payments slip.

For the purpose of this clause:

"Legal Name" means the name of the company, corporation or other entity constituted as a legal person under which this person exercises its rights and performs its obligations.

"Operating Name" means the name that is legally protected and used in the course of its business by a company, corporation or other entity legally constituted as a legal person, or by the individual.

The Bidder is requested to provide the following:

Legal Name:

Operating Name: _____

Address: _____

_____

Payment/T1204 Address (if different)   ☐ Payment address is same as above

_____

_____

City: _____

Province: _____

Postal Code: _____

Telephone: _____

Fax: _____

Type of Business (Select only one)

☐ Corporation   ☐ Partnership   ☐ Sole Proprietor   ☐ Non-Profit Organization   ☐ US or International Co.

All registered companies (excluding Non-Profit organizations and US or International companies) must provide their Goods and Services Tax (GST) or Business Number (BN). Additional details on how to obtain a BN can be found at: http://www.cra-arc.gc.ca/tx/bsnss/tpcs/bn-ne/menu-eng.html

If the services will be rendered by an individual, please provide the Social Insurance Number (SIN).

Goods and Services Tax (GST) Number: _____

Business Number (BN):

_____

_____

If a SIN number is being provided, the
information should be place in a sealed
envelope marked "Protected".

Social Insurance Number (SIN):

☐ N/A Reason:

_____

_____

Note: If you select "N/A", then you must give a reason.

Date: _____

Name: _____

Signature: _____

(Signature of duly authorized representative of business)

Title: _____

(Title of duly authorized representative of business)

PART 6:   SECURITY 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 - Model Contract;

    b)   the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirements as indicated in Part 7 - Model Contract;

    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 address(es) of proposed site(s) or premises of work performance and document safeguarding.

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.

APPENDICES

Appendix 1: Mandatory Criteria

Evaluation Procedures

Bids will be evaluated in accordance with the process outlined in Part 4 Evaluation and Selection and all the mandatory evaluation criteria detailed below. The Bidder must provide supporting documentation in its bid as requested by CRA, in order to demonstrate that each technical mandatory requirement has been met. To assist with the evaluation process, it is preferred that the Bidder complete the table included below, to indicate where in its bid the information can be located. Bids that fail to meet all mandatory requirements will be declared non-responsive and the bid will receive no further consideration.

ID	Mandatory Requirement Description	Bidders Substantiation of Requirement
M1	The EMNSS proposed to meet this requirement must be off-the-shelf, meaning that each component of the EMNSS is commercially available and requires no further research and development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment).	
M2	The provider must have delivered an EMNSS as a hosted application for at least three years.	
Service architecture requirements		
M3	Service Design: The EMNSS must be designed specifically for emergency notifications with the capability of broadcasting mass notifications to multiple users within 15 minutes.	
M4	Call Throttling: The EMNSS must have the ability to control the number of calls into an organization to avoid flooding the lines during a mass notification.	
M5	Proprietorship: All hardware, software and data (apart from client's owned systems) must be hosted at facilities owned or leased, operated and secured in Canada.	
Requirements for Client Operation		
M6	Platform: The EMNSS must not require the use of plug-ins for any functionality.	
M7	The client must not be required to install any hardware or software to operate any facets of the EMNSS. Database capacity, data channels and phone ports are not purchased by the client.	
M8	HotLine: The EMNSS must be able to transfer the current CRA Building Status toll free phone number to their system.	
Security requirements		
M9	Encryption: The Bidder must employ Communications Security Establishment Canada (CSEC) https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111 approved cryptography to protect sensitive data. The EMNSS user credentials for web console access (if equipped) must be encrypted in transit using the Transport Layer Security (TLS) version 1.2 or above.	
M10	The EMNSS must provide mechanisms to protect the authenticity of communications sessions.	
M11	The EMNSS must protect the confidentiality and integrity of information at rest.	

ID	Mandatory Requirement Description	Bidders Substantiation of Requirement
M12	The EMNSS must provide a facility for CRA to define role-based access to the data and functions of the EMNSS.	
M13	Access Privileges: The EMNSS must enable Administrators to control access privileges, such as access requests, requests for changes to personal information, and changes to passwords, provided that they have appropriate access control permissions.	
M14	Password Change: The EMNSS must permit each Administrator and user to change their password at any time.	
M15	Password Strength: The EMNSS must force each Administrator and user to configure a password in a predetermined manner with a minimum number of characters, including capitals, numbers and symbols.	
M16	The EMNSS must use replay-resistant authentication mechanisms for access to the system.	
M17	The EMNSS must obscure feedback of authentication information during the authentication process.	
M18	The EMNSS must allow Administrators to define and enforce a limit of invalid authentication attempts within a given time period. When the threshold has been met the information system locks the account until released by the administrator.	
M19	Session Lock: The EMNSS initiates a session lock after an Administrator defined time period of inactivity. The information system retains the session lock until the user re-establishes access by re-authenticating.	
M20	The EMNSS must protect against or limits the effects of denial of service attacks.	
M21	The EMNSS must protect the integrity of transmitted information based on the CSEC approved communication algorithms https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111.	
M22	Malicious Code Protection: The EMNSS must employ malicious code protections at all system entry and exit points, at workstations, servers, and/or mobile computing devices on the network to detect and eradicate malicious code on the system. The code protections (including signature definitions) should be updated whenever new releases are available. Regular scans of the information system are conducted daily and real-time scans are performed as files are downloaded, opened or executed in order to ensure that malicious code is detected, eradicated, and quarantined.	
Audit and Accountability		

M23	The EMNSS must audit the following events:
	   i. System Administrator access to the application
	   ii. General user access to the application
	   iii. Database maintenance activities
	   iv. Application configuration changes	

M24	The audit records produced by the EMNSS must contain sufficient information to:
	   i. Identify the type of event that occurred
	   ii. The date and time at which the event occurred
	   iii. Where the event occurred
	   iv. The source of the event
	   v. The outcome of the event	

ID	Mandatory Requirement Description	Bidders Substantiation of Requirement
M25	The EMNSS must ensure that sufficient storage capacity is available to prevent loss of audit records due lack of capacity. When maximum storage capacity of audit records has been reached the Bidder will notify the CRA administrator. The audit logs must be kept for a period of two years.	
M26	The EMNSS must use internal system clocks to generate timestamps for audit records and that underlying servers use an authoritative time source (such as an Network Time Protocol (NTP) http://www.ntp.org/) to synchronize their clocks weekly.	
M27	The EMNSS must ensure that access to audit records can be limited based upon the role based access permissions (for example, Administrators can view but not create, modify, or delete audit records while other users do not have access to the audit records).	
M28	The EMNSS must protect audit records and ensures that audit information is backed up and retained for a period of two years.	
Retention and destruction of records		
M29	Users information records must be purged from the system immediately after the user unsubscribes from the system (i.e. no second copies of data are to be stored unless known to and authorized by the CRA). Purged data must not be recoverable.	
M30	The Administrators must have the ability to delete all transitory records.	
M31	At the conclusion of the contract and/or at the request of the CRA, all CRA related information must be removed, and securely deleted from the EMNSS. The secure destruction of the data must be conducted in such a manner that no recovery can be performed. A letter of certification must be provided confirming destruction of all CRA data.	
Resiliency requirements		
M32	Recovery: Client data must be hosted in high-availability facilities with zero fail-over time and automatic recovery.	
M33	Disaster Recovery: If a disaster, emergency or hazard renders the EMNSS primary data centre inoperable, client data must be dynamically rerouted so that it functions without interruption.	
M34	Back-Up Facilities and Services: The EMNSS must have a multi-tier, multi-server fault tolerant architecture with full redundancy whereby the users contact information database server and all EMNSS functions are housed in Canada and their back-up capability is housed in separate locations in Canada separated by a provincial boundary (at least 200 km) so that an emergency that affects one facility will not affect the others.	
M35	Location of Data Servers: The EMNSS must ensure that the client's database never resides outside of Canada's land boundaries.	
M36	Permissions and Access Controls: The EMNSS must enable and support the designation of a minimum of 10 Master Administrators with full access, Regional and Local (building) Administrators with limited access.	
General operations requirements		
M37	User Interfaces: The EMNSS must provide graphical user interfaces (GUI) in both English and French for all users.	
M38	Browsers: The EMNSS must be accessible to Administrators and users on web browsers including Internet Explorer (min version 9.0), Microsoft Edge, Apple Safari (min version 5.1), Google Chrome (min version 17.0) and Mozilla Firefox (min version 10.0) for Windows - and compatible with 128-bit encryption.	

ID	Mandatory Requirement Description	Bidders Substantiation of Requirement
M39	Quick Launch: The EMNSS must have a quick-launch feature that allows an Administrator to initiate a message from a single screen after logging in to the EMNSS.	
M40	Practice Modes: The EMNSS must have practice modes (i.e., a test environment) that allow the Administrators to use any facet of the EMNSS without affecting real-time content or capabilities of the EMNSS and the database (i.e., the production environment).	
M41	Self-Registration: The EMNSS must allow to self-register and update their own profile information at any time.	
M42	Mapping: The EMNSS must have a map function to select a radius surrounding an event for notifications to be sent to only the selected geographic area.	
Output		
M43	Voice Messages: The EMNSS must send local or long-distance voice messages of up to 1 minute in duration (exclusive of dialing time, ringing time and voice-mail response time).	
M44	Voice Message Language: Voice messages must be delivered with voices using Canadian English and Canadian French.	
M45	Text-based Messages: The EMNSS must send text-based SMS messages of a minimum of 140 characters or e-mail messages of up to 500 words to at least 13000 registered users within 10 minutes of being sent.	
M46	Reliability: The EMNSS must be fully functional and operational 24 hours a day, 7 days a week, with at least 99.99% availability throughout the Contract period. In the event of an outage, the EMNSS provider will advise the client within 30 minutes of the outage and the impacts on the EMNSS.	
M47	Reliability: In the event of a scheduled outage, the Bidder will advise the client at least 5 business days in advance of the outage.	
M48	Support: The EMNSS must offer technical support 24 hours a day, 7 days a week.	
M49	Native SMS in Canada: The EMNSS must use short code (5 digits number) in order to allow for the sending of true SMS versus email-to-SMS.	
Database		
M50	Data Recovery: The EMNSS must enable Administrators to recover a user contact record that has been deleted for up to 5 days after deletion.	
M51	Database Backup: The EMNSS must generate automatic database backups to one or more other locations in Canada at least once every 24 hours.	
User Information		

M52	Administrator and User Profiles: The EMNSS must allow for the establishment and maintenance of a database of Administrator and user profiles that include the following:	
	i. Full name	
	ii. Region	
	iii. Branch	
	iv. Business address	
	v. Home address	
	vi. Cell phone number	
	vii. Home phone number	
	viii. Business phone number	
	ix. Personal e-mail address	
	x. Work e-email address	
	xi. Designated alternate	
	xii. Permissions assigned	
	xiii. Master Administrators must have full access permissions to perform all functions of the EMNSS.	
M53	User Information Data Fields: The EMNSS must enable Administrators to identify mandatory data fields.	
M54	User Information Data Fields: The EMNSS must accommodate the creation of 25 data fields per record.	
M55	Data Revision: The EMNSS must enable Administrators and users to view and manually edit the information in their own profiles, directly within the EMNSS, provided they have appropriate access control permissions.	
M56	Data Revision: The EMNSS must enable Administrators and users to add, modify, and delete user information, directly within the EMNSS, provided they have appropriate access control permissions.	
Groups		
M57	Creation: The EMNSS must enable Administrators to create groups based on variables such as Region, Building or other criteria identified in the data fields of each user's record.	
M58	Hierarchical Groups: The EMNSS must enable Administrators to create hierarchical groupings so that groups include up to 30 levels of sub-groups in order to appropriately reflect an organization's structure.	
M59	Number of Groups: The EMNSS must enable Administrators and users to define a user to be a member of up to 50 groups.	
Message initiation		
M60	Service Access: The EMNSS must enable Administrators to access the service for user management, message creation (voice or text-based) or message transmission purposes via the following methods and devices:	
	i. Computer (via the internet either through cable or WI-FI or Voice over Internet protocol);	
	ii. Landline telephone;	
	iii. Cellular telephone;	
	iv. Teletype device (TTY); and	
	v. EMNSS Application.	
M61	Message Creation: The EMNSS must enable Administrators to create and save templates in French and English.	
M62	Message verification: Administrators must be able to hear the voice message and/or to read the text-based message before it is sent. Administrators must be able to edit or rerecord the message if it was not correct.	
M63	Time Zone Recognition: The EMNSS must recognize and process to the relevant time zones for notifications that are sent from a time zone, but delivered to another time zone.	
Message transmission		

M64	Media: The EMNSS must send messages to users via the following:
	   i. Landline telephone;
	   ii. Cellular telephone;
	   iii. SMS text message;
	   iv. E-mail;
	   v. Teletype device (TTY); and
	   vi. EMNSS Mobile Application (push notifications).	

M65	Safeguards: The EMNSS must have an effective safeguard (such as a prompt message) that prevents routine messages from being sent out as emergency notifications.	
M66	Phone Number Types: The EMNSS must have the ability to make local and long distance calls within Canada.	
M67	Order of Contact Methods: The EMNSS must enable Administrators and users to set the default order of devices used to notify users.	
M68	Language of Message: The EMNSS must enable Administrators to create messages in French and English and to automatically transmit them in the user's pre-selected corresponding language.	
M69	Simultaneous Transmission: Administrators must be able to send a recorded voice message and a text message in a single notification to all selected users for delivery through the media listed in **M64**.	
M70	Caller ID: Either globally or on a message-by-message basis, the EMNSS must enable Administrators initiating a message to customize the telephone number displayed (caller ID) for voice messages and the e-mail addresses for text-based messages.	
M71	Escalation: The EMNSS must escalate messages when the intended user has not confirmed receipt of the correspondence (with 3 levels of escalation) within a given period of time.	
M72	Delivery Attempts: Administrators must be able to select the number of delivery attempts through all contact method paths.	
M73	E-mail Attachments: The EMNSS must be able to attach multiple files (e.g. text, spreadsheet and images) to e-mails.	
M74	Message Control: Administrators must be able to stop, recall or replace a message initiated by them or another Administrator with the same or higher level of permissions at any time during the message sending process.	
M75	Designated alternate: The EMNSS must automatically send messages to a designated alternate (if one has been designated) if a user does not acknowledge receipt of the initial message within a period of time defined by the sender.	
M76	First to Respond: The EMNSS must have the capability to send notifications systematically until a predetermined number of affirmative responses are received.	
M77	Roll Call: The EMNSS must have the capability to send notifications for the purpose of soliciting an acknowledgement from the recipient..	
M78	HotLine: When calling the EMNSS hotline, users must only obtain notifications pertaining to the individual work site(s) they have registered for (physical building location). Users are not to obtain or have to listen to any notifications for other work sites they have not registered for.	
Message delivery features		
M79	Voice Message Repeat: The EMNSS must allow the users to listen to a voice message as often as desired with a single key press.	
M80	Voice-Mail: The EMNSS must leave a message when a voice-delivered message reaches an answering machine or voicemail. If a message is left, the EMNSS must also contact the next contact method if the message was left on the primary contact method.	
Message management		
M81	Scheduling: The EMNSS must enable Administrators to schedule a notification to be sent at a future date and time.	

M82	Mass notifications: The EMNSS must have unlimited and unrestricted mass notifications capabilities.

Reporting	
M83	Dashboard: The EMNSS must provide a real-time dashboard for each active notification broadcast allowing Administrators to view broadcast parameters (e.g. devices, start time, duration and number of cycles) and see status of broadcast results (e.g. delivery confirmation).
M84	History: The EMNSS must enable Administrators to view a history of message results for the entire period of the contract.
M85	Audit Trail: The EMNSS must produce real-time message broadcast result reports using all application data which contains, but is not limited to, all of the following information: i. Name, date and time of the message; ii. Name of the Administrator or user who initiated the broadcast; iii. Summary statistics, including total notified users, total confirming receipt/not confirming receipt, percentage confirming receipt/not confirming receipt. This information must be collated for individual messages and cumulatively; and iv. Detailed calling information, including call-result of each attempt within the broadcast, the addresses and associated phone numbers attempted, the attempt number and the result (e.g., confirmed with date and time, busy, no answer or voicemail).
M86	Export: The EMNSS must export all types of report data in CSV, XLS, HTML, or PDF formats, as defined by an Administrator or user.
M87	Printing: The EMNSS must enable Administrators to print real-time reports of any data or statistics directly from the GUI.
M88	Reports: Upon request, the Bidder must search and generate reports based on user-defined criteria and/or key words including wild card searches. In addition, the Bidder must retain, on their servers, a record of all reports for the entire period of the contract.

Training	
M89	The Bidder must provide in-house training on CRA premises.
M90	The EMNSS must be supplied with manuals downloadable from the Internet.
M91	The EMNSS manuals must define all functions and include complete instructions for the operation of the product.

Appendix 2: Financial Bid

The Bidder must submit their financial bid in accordance with the Financial Proposal hereafter.

Bidders must submit firm prices for unlimited users in Canadian funds, Canadian customs duties and excise taxes included, and Applicable Taxes excluded, Delivered Duty Paid (DDP) (Ontario), for the provision of goods and services outlined in Annex A "Statement of Requirement".

The prices specified include all of the requirements defined in the "Statement of Requirement" in Annex A.

PART 7:   Model Contract

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT

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

7.1   Revision of Departmental Name

Reference to the Minister of Public Works and Government Services or to Public Works and Government Services Canada contained in any term, condition or clause of the contract shall be interpreted as a reference to the Commissioner of Revenue or the Canada Revenue Agency, as the case may be, with the exception of the following clauses:

a) Standard Clauses and Conditions; and
b) Security Requirements.

7.2   Agency Restructuring

In cases where the Contracting Authority's department or agency is being reconfigured, absorbed by another government department or agency, or disbanded entirely, the Commissioner may, by giving notice to the Contractor, designate another Contracting Authority for all or part of the Contract.

7.3   Requirement

The Contractor must perform the Work in accordance with the Statement of Requirements (SOR) at Annex A, attached hereto and forming part of the Contract

7.4   Period of the Contract

The period of the Contract is from the date the contract is awarded to three (3) years later.

7.5   Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 7 (seven) additional one-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.

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

7.6   Option to Purchase Additional Quantities of the Goods, Services or Both

The Contractor grants to Canada the irrevocable option to acquire the additional quantities of the goods, services or both described at Annex B, Basis of Payment of the Contract under the same terms and conditions and at the prices and/or rates stated in the Contract.

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

7.7   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 issued by Public Services and Procurement Canada (PSPC).

The Manual is available on the PSPC Website: https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual

The following Clauses are incorporated by reference:

SACC Reference	Clause Title	Date
A2000C	Foreign Nationals (Canadian Contractor) OR	2006-06-16
A2001C	Foreign Nationals (Foreign Contractor) *(to be determined at contract award)*	2006-06-16
A3015C	Certifications – Contract	2014-06-26
A9068C	Government Site Regulations	2010-01-11
A9117C	T1204 – Direct Request by Customer Department	2007-11-30
B9028C	Access to Facilities and Equipment	2007-05-25
C2000C	Taxes – Foreign-based Contractor (*To be deleted at contract award if not applicable.*)	2007-11-30
C6000C	Limitation of Price	2011-05-16
C2605C	Canadian Customs Duties & Sales Tax –Foreign-based Contractor	2008-05-12
G1005C	Insurance	2008-05-12
H1000C	Single Payment	2008-05-12
H3028C	Advance Payment	2010-01-11

7.8   General Conditions

2030 (2016-04-04) General Conditions – Higher Complexity - Goods, apply to and form part of the Contract.

Section 01 titled "Interpretation" the definition of "Canada", "Crown", "Her Majesty" or "the Government" is hereby amended to read: "Canada", "Crown", "Her Majesty" or "the Government" means Her Majesty the Queen in right of Canada as represented by the Canada Revenue Agency (CRA).

Section 02 titled "Standard Clauses and Conditions" is hereby amended to delete the phrase "Pursuant to the Department of Public Works and Government Services Act, S.C. 1996, c. 16," The remainder of Section 02 remains unchanged.

Section 23 titled "Confidentiality",

> Subsection 5 is hereby amended to delete Public Works and Government Services (PWGSC) and insert Canada Revenue Agency (CRA).

> Subsection 6 is hereby amended to delete "PWGSC Industrial Security Manual and its supplements", and insert "Security Requirements for the Protection of Sensitive Information" issued by the CRA, Security and Internal Affairs Directorate (SIAD). The remainder of Section 23 remains unchanged.

Section 43 titled "Integrity Provisions- Contract" is hereby deleted in its entirety and replaced with:

The Supplier Integrity Directive (SID) incorporated by reference into the bid solicitation is incorporated into, and forms a binding part of the Contract. The Contractor must comply with the provisions of the SID, which can be found on the Canada Revenue Agency's website at *https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/procurement-cra/supplier-integrity-directive.html*.

Section 45 titled "Code of Conduct for Procurement—Contract" is hereby deleted in its entirety.

7.9   Supplemental Terms and Conditions

4003 (2010-08-16), Supplemental General Conditions - Licensed Software, modified as follows, shall apply to and form part of the Contract.

At section 1 titled "Interpretation" insert the following definition:

The "Licensee" under the Contract is Her Majesty the Queen in right of Canada, acting through and represented by the Commissioner, Canada Revenue Agency.

At section 2 titled "License Grant" delete subsection 2 and replace with the following:

If the Client is reconfigured, absorbed, in whole or in part, by another government department or agency, or is disbanded entirely, Canada may, by giving notice to the Contractor, designate another department or agency as the Client for all or part of the Licensed Software.

At section 08 titled "Licensed Software Transfer", delete this article in its entirety and replace with the following:

The license to use the Licensed Software under the Contract is transferable by Canada, in whole or in part, under the same conditions of the Contract, to any Device or Client, as applicable, or to any Canadian government department, corporation or agency, as defined in the *Financial Administration Act, R..S. C.1985, c.F-11*, as amended from time to time, or to any other party for which the Department of Public Works and Government Services   Canada has been authorized to act under section 16 of the *Department of Public Works and Government Services Act, S.C. 1996, c.16,* as long as Canada informs the Contractor of the transfer within thirty (30) days of the transfer occurring.

At Section 11 titled "Term of License" delete subsection 2 and replace with the following:

The Contractor may terminate Canada's license with respect to the licensed software by giving the Contracting Authority written notice to that effect only if Canada is in breach of its license in accordance with the license rights granted in the Contract, or Canada fails to pay for the license in accordance with the Contract, and only if that breach continues for a period of ninety (90) days after the Contracting Authority received written notice from the Contractor giving particulars of the breach and the Contracting Authority has validated the particulars of the breach. If Canada's license is terminated, once Canada has corrected the breach, the Contractor shall re-instate Canada's license with respect to the licensed software under the exact same terms and conditions as granted in the contract for the license, at no additional cost.

At section 15 titled "Warranty", insert the following:

Notwithstanding section 15.0 – Warranty, the Contractor's warranty for the Solution shall include the provision of all software maintenance and support services detailed in supplemental general conditions 4004 – Support Services for Licensed Software except that "Warranty Period" as defined therein is hereby amended by deleting the reference to a period of ninety (90) days and replacing ninety (90) days with one (1) year. The warranty period of twelve (12) months shall commence on the final acceptance date of the delivered Equipment.

Section 18 titled "Risk of Loss" insert the following after subsection 2:

     3.   The Contractor warrants:

Unless authorized in writing by the Technical Authority, or necessary to perform valid duties under the Contract any programs developed by the Contractor under the Contract or provided to Canada by the Contractor for use by the Client shall:

i.   not replicate, transmit, or activate itself without control of the person operating the computing equipment on which it resides;

ii. not alter, damage, or erase any data or computer programs without control of a person operating the computing equipment on which it resides; and

iii. contain no key, node lock, time out or other function, whether implemented by electronic, mechanical or other means, which restricts or may restrict use or access to any programs or data developed under the Contract, based on residency on a specific hardware configuration, frequency or duration of use, or other limiting criteria.

Provided and to the extent any program has any of the foregoing attributes, and notwithstanding anything elsewhere in the Contract to the contrary, the Contractor shall be in default of the Contract, and no cure period shall apply. In addition to any other remedies available to it under the Contract, the Crown reserves the right to pursue any civil and/or criminal penalties available to it against the Contractor. The Contractor agrees, in order to protect the Crown from damages, which may be intentionally or unintentionally caused by the introduction of Illicit Code to the Client's computer network, no software will be installed, executed, or copied on Client equipment without the express approval of the Technical Authority.

4004 (2013-04-25), Supplemental General Conditions - Maintenance and Support Services for Licensed Software, shall apply to and form part of the Contract.

7.10   Software License Type

The Contractor hereby grants a 3 year subscription to Her Majesty the Queen in right of Canada for the software listed in Annex A.The term "User" and "User License" shall have the meanings set out in supplemental general conditions 4003 (2010-08-16), Licensed Software.

7.11   License Terms and Conditions – Shrink-Wrap or Click

The parties agree that only the conditions expressly set out in the Contract or incorporated by referenced in the Contract form part of the Contract. Any conditions accompanying or enclosed with the Licensed Software, if any, do not form part of the Contract and, therefore, are not part of Canada's license and do not affect the rights of the Parties in any way. The Contractor agrees that in no event will Canada or any Client or User be required to enter into any additional license agreement with respect to the Licensed Software or any portion of it. The Contractor acknowledges that any additional license agreement relating for the Licensed Software signed by anyone other than the Contracting Authority is void and of no effect.

Canada is not bound by and does not accept any "shrink-wrap" or "click-wrap" conditions or any other conditions, expressed or implied, that are contained in or on the software packaging or conditions that may accompany the software in any manner, regardless of any notification to the contrary.

7.12   Maintenance

The Contractor shall inform the Technical Authority within 2 business days of the availability of all enhancements, product upgrades and maintenance releases to the Software during the period of service. All generally available enhancements must either be made available for download or shipped to CRA within one (1) business day of a request by CRA.

7.13   Documentation and Technical Manuals

The Contractor shall deliver a total of 1 copy in print and 1 copy in electronic format of all technical, installation and operations manuals for the Solution. These manuals must be provided in hard copy format and if available, manuals must also be provided on CD or softcopy, in either MS Word or PDF formats. Documentation must be accessible through the Contractor's web-site or OEM web-site, and URL must be provided.

The Contractor will provide Canada with the right to reproduce for its own use and incorporate into any documents produced for its own use any commercially available documentation delivered under the Contract. The Contractor shall further secure and agree to extend the same rights for all future revisions of the said documentation and material supplied to Canada. Any document or material that is translated by Canada shall include any copyright and any proprietary right notice that was part of the original document.

The Contractor shall deliver a complete set of documentation in French, if available. If documentation is not available in French CRA shall have the right to translate the documentation and material delivered herein into the second of the two Official languages of Canada. This right shall include the right to make, or to have made, copies for CRA's internal purposes only. The Contractor acknowledges that CRA owns the translated version of any such translated document and material and that it is under no obligation to provide any translated document or material to the Contractor. Any document or material that is translated by Canada shall include any copyright and any proprietary right notice that was part of the original document. Canada acknowledges that the Contractor is not responsible for technical errors that arise as a result of any translation performed by CRA.

7.14 Security Requirements

Security Requirements - Document Safeguarding and/or Production Capabilities – with Computer Systems

1.   The Contractor personnel requiring access to Protected information, assets or sensitive work site(s) must each hold a valid Reliability screening, granted by the Security and Internal Affairs Directorate (SIAD) of the Canada Revenue Agency (CRA) or the Canadian and International Industrial Security Directorate (CIISD) of Public Services and Procurement Canada (PSPC).

2.   The Contractor must not remove any Protected information or assets from the identified and approved work site(s), and the Contractor must ensure that its personnel are made aware of and comply with this restriction.

3.   The Contractor shall, at all times during the performance of the Contract, hold an approved facility clearance for Document Safeguarding at the Protected A level issued or granted by CIISD or a letter issued by the SIAD confirming that the facility is approved and meets the CRA security requirements.

4.   Processing of material only at the Protected A level is permitted under the Contract. Protected A information can be stored on cloud based systems providing the Contractor demonstrates their ability to protect data in accordance with the Document safeguarding capabilities (DSC) for Protected A.

5.   Subcontracts which contain security requirements are not to be awarded without the prior written permission of CRA.

6.   The Contractor must comply with the provisions of the:
·   Security Requirement Check List (SRCL), attached as Annex C of the contract; and
·   Security Requirements for Protection of Sensitive Information issued by CRA, Security and Internal Affairs Directorate.

These may be viewed at: Security Requirements

7.15 Authorities

7.15.1 Contracting Authority

The Contracting Authority for the Contract is:

Name: Alastair Webb
Telephone Number: 613-867-5203
E-mail address: Alastair.webb@cra-arc.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.

7.15.2 Technical Authority

To be completed at the time of Contract award.
Name:
Address:
Telephone Number:
Fax Number:
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.

7.15.3 Contractor's Representative

To be completed at the time of Contract award.
Name:
Address:
Telephone Number:
Fax Number:
E-mail Address:

7.16 Contractor Identification Protocol

The Contractor must be responsible for ensuring that each of its employees, officers, directors, agents, and subcontractors (hereinafter referred to as "Contractor Representative") complies with the following self-identification requirements:

A Contractor Representative who attends a Government of Canada meeting whether internal or external must identify themselves as being a representative of the Contractor prior to the commencement of the meeting to ensure that each meeting participant is aware of the fact that the individual is not a government employee;

During the performance of any Work at a Government of Canada site, each Contractor Representative must be clearly identified at all times as being a Contractor Representative; and

If a Contractor Representative requires the use of the Government of Canada's e-mail system in the performance of the Work, then the individual must clearly identify themselves as a non-government employee in all electronic mail in the signature block as well as under "Properties".

This identification protocol must also be used in all other correspondence, communication and documentation.

7.17 Travel and Living Expenses

The CRA will not cover any travel and living expenses.

7.18 Work Location

The work location will be at 250 Albert Street, Ottawa, ON, K1A 0L5.

7.19 Sustainable Development

In pursuit of the Canada Revenue Agency's commitment to sustainable development and green procurement as well as the Canadian Federal Government's Green Procurement Policy, the Contractor agrees to commit to comprehensive, nationally recognized environmental standards for:

- The reduction or elimination of environmentally hazardous materials (if applicable);
- Design for reuse and recycle;
- Energy efficiency;
- End of Life Management for reuse and recycle;
- Environmental stewardship in the manufacturing process (if applicable); and
- Packaging.

7.20 Delivery

For the initial order of software licenses the Contractor must make the complete delivery to the Technical Authority within ten (10) business days from the date of Contract award.

For orders made on an "as and when requested" basis the Contractor must make complete delivery within ten (10) business days from receipt of an order.

For orders to procure professional services made on an "as and when requested" basis the Contractor must make complete delivery in accordance with the timeframes contained in the associated Contract Amendment.

7.21 Inspection and Acceptance

All deliverables under the Contract shall be subject to inspection and acceptance by the Technical Authority at destination.

7.22 Basis of Payment

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid firm annual prices, as specified in Annex B, Basis of Payment. Customs duties are included and Applicable Taxes are extra.

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

7.23 Maintenance and Support Pricing Stability

Unless otherwise stated in the Contract subsequent annual maintenance and support prices beyond the effective periods of the maintenance and support pricing in Annex B, List of Deliverables and Pricing, shall not exceed the lesser of:

a. The Contractor's current published maintenance rate in effect at time of renewal; or
b. The previously contracted rates for each item, adjusted by the % change in the Core Consumer Price Index (CPI) for Canada, not seasonally adjusted and calculated from the corresponding month of the previous year, as published by Statistics Canada on the date the maintenance renewal is issued; or
c. Any other negotiated rate.

7.24 Training of Contractor Personnel

Any training required by a new or replacement resource will be the responsibility of the Contractor, including training the resource for newly implemented software. The Contractor will assume all associated costs, including training pertaining to familiarization during the start-up of the Contract and Contract period for staff replacements. Training of the resource during the start-up period must take place without a reduction in service level. Time spent on such training will not be billed to, nor paid by, CRA.

7.25 Familiarization Period

Prior to the completion of the Contract, it may be necessary for another resource to undertake a period of familiarization and training before the completion date. The Contractor will be required to familiarize the incoming

resource according to the process described above or through the use of another approach negotiated with and acceptable to CRA.

7.26   Payment Process

At Canada's discretion the Contractor will be paid using direct deposit or cheque. All communications regarding the specific method of payment, including changes thereto, will be in writing via email as it's not Canada's desire to formally amend the Contract if the payment method is changed.

At its sole discretion Canada may change the method of payment at any time during the period of the Contract, including any extension thereto, to one of the other two payment methods stated above.

It is the sole responsibility of the Contractor to ensure that their organization is entitled to receive payment from the Government of Canada.

7.26.1   Payment by Direct Deposit

The Contractor shall accept Direct Deposit for payment of the goods and/or services described herein. Payments by direct deposit will be subject to Article 18 – Payment Period and Article 19 - Interest on Overdue Accounts, set out in 2030General Conditions (2016-04-04) forming part of the Contract.

To complete or amend a direct deposit registration, the Contractor must complete the Vendor Electronic Payment Registration form accessible at: http://www.cra-arc.gc.ca/E/pbg/tf/rc231/rc231-14e.pdf

It is the sole responsibility of the Contractor to ensure that the information and account number submitted to Canada via their Vendor Electronic Payment Registration form is up to date. Should the Contractor's information within the Vendor Electronic Payment Registration form not be accurate or up to date, the provisions identified herein under Article 18 – Payment Period and Article 19 - Interest on Overdue Accounts, set out in 2030 General Conditions (2016-04-04) forming part of the Contract will not apply, until the Contractor corrects the matter.

7.26.2   Payment by Cheque

The Contractor shall accept Government of Canada cheques for the payment of goods and/or services described herein.

7.27   Refund to the Crown in the Event of Termination

Notwithstanding Article 32 of 2030 (2016-04-04), "Termination for Convenience", General Conditions – Higher Complexity - Goods, in the event of termination of services for which an advance payment has been made, charges up to the date of termination will be calculated by prorating on the basis of a twelve (12) month year and a thirty (30) day month, and the Contractor shall immediately refund to Canada the unliquidated portion of the advance payment.

7.28   Invoicing Instructions

The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the General Conditions.

   a)   The original and one (1) copy must be forwarded to the Technical Authority of the Contract identified under the section entitled "Authorities" for certification and payment.
   b)   One (1) copy must be forwarded to the Contracting Authority of the Contract identified under the section entitled "Authorities"

7.29 Certifications

The continuous compliance with the certifications provided by the Contractor in its bid and the ongoing cooperation in providing associated information are conditions of the Contract. Certifications are subject to verification by Canada during the entire period of the contract. If the Contractor does not comply with any certification, fails to provide the associated information, or it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

7.30 Federal Contractors Program for Employment Equity – Default by the Contractor

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC) - Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE becomes invalid, the name of the Contractor will be added to the "FCP Limited Eligibility to Bid" list. The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

7.31 Joint Venture (NOTE to bidders: to be deleted at contract award if not applicable)

If the Contract is awarded to a joint venture, all members of the joint venture will be jointly and severally or solidarily liable for the performance of the Contract.

In the case of a contractual joint venture, no dispute, claim or action for damages, whether based in contract, or in tort, or any other theory of law, howsoever arising from the Request for Proposal, Contract, or any other related or subsequently issued documents including without limitation Task Authorizations, Contract Amendments, may be commenced, or brought against the CRA, including without limitation any of its officers, employees or agents unless each member of the joint venture is a party to such dispute, claim, or action (as the case may be).

The Contractor shall obtain the prior written approval of the Contracting Authority to any change in the membership of a contractual joint venture after Contract Award. Any change in the membership of a contractual joint venture after Contract Award without the prior written approval of the Contracting Authority shall be deemed to be default under the Contract.

The joint venture represents and warrants that it has appointed and granted full authority to _____ *(name to be inserted at Contract Award)*, the "Lead Member", to act on behalf of all members as its representative for the purposes of executing documentation relating to the Contract, including but not limited to Contract Amendments and Task Authorizations.

In the event of a contractual joint venture, all payments due and owing to the joint venture shall be made by the Canada Revenue Agency to the Lead Member of the joint venture. Any such payment to the Lead Member of the joint venture shall be deemed to be payment to the joint venture and shall act as a release from all the members of the joint venture.

By giving notice to the Lead Member the Canada Revenue Agency will be deemed to have given notice to all the members of the joint venture.

7.32 Applicable Laws

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

7.33 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 ha priority over the wording of any document that subsequently appears on the list.

1. The Articles of Agreement;
2. The Supplemental General Conditions 4003 (2010-08-16), Licensed Software;
3. The Supplemental General Conditions 4004 (2013-04-25), Maintenance and Support for Licensed Software;
4. The General Conditions 2030 (2016-04-04);
5. Annex A: Statement of Requirement;
6. Annex B: Basis of Payment;
7. Annex C: Security Requirements Check List (SRCL);
8. The Contractor's proposal dated (insert date of bid), as amended on (insert date(s) of amendment(s), if applicable).

7.34 Alternative Dispute Resolution

NEGOTIATION FOLLOWED BY MANDATORY MEDIATION, THEN, IF NECESSARY BY ARBITRATION OR LITIGATION

The parties agree to meet, negotiate in good faith, and attempt to resolve, amicably, any dispute arising out of or related to the contract or any breach thereof.

If the parties are unable to resolve the dispute through negotiations within 10 working days, the parties agree to attempt to resolve the dispute through mediation by submitting the dispute to a sole mediator selected jointly by the parties. All costs shall be shared equally between the disputing parties.

If a dispute cannot be settled with a 15 calendar day period after the mediator has been appointed, or if the parties are unable to select a mediator within 15 calendar days of the date of provision of notice by one party to the other of the intention to proceed to mediation, or such longer period as agreed to by the parties, the parties shall have the right to resort to any remedies permitted by law, including but not limited to arbitration or litigation.

All defences based on the passage of time shall be tolled pending the termination of the mediation.

7.35 Limitation of Liability

1. This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this section, even if it has been made aware of the potential for those damages.

2. First Party Liability:

    a. The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:

        i. Any infringement of intellectual property rights to the extent the Contractor breaches the section of the general conditions entitled "Intellectual Property Infringement and Royalties";

        ii. Physical injury, including death.

b. The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.

c. Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

d. The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (a) above.

e. The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

   i. any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including Applicable Taxes) for the goods and services affected by the breach of warranty; and

   ii. any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (ii) of the greater of the total estimated contract cost (meaning the dollar amount shown on the first page of the Contract in the block titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or $1 Million,

   whichever is greater.

   In any case, the total liability of the Contractor under paragraph (e) will not exceed the total estimated cost (as defined above) for the Contract or $1 Million.

f. If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

3. Third Party Claims:

a. Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.

b. If Canada is required, as a result of joint and several liability, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite paragraph (a), with respect to special, indirect, and consequential damages of third parties covered by this section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual

property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.

c. The Parties are only liable to one another for damages to third parties to the extent described in this paragraph 3.

7.36 Intellectual Property Right Infringement

1. If a third party claims that equipment or software that the Contractor provides under the Contract infringes any intellectual property right, the Contractor, if requested to do so by Canada, will defend Canada against the claim at the Contractor's expense. In this regard, the Contractor will pay all costs, damages and legal fees that a court finally awards, provided that Canada:

   a. promptly notifies the Contractor in writing of the claim; and

   b. co-operates with the Contractor in, and allows the Contractor full participation in, the defense and related settlement negotiations; and

   c. obtains the Contractor's prior approval to any agreement resulting from settlement negotiations held with the third party.

2. The Contractor shall participate in any claims, action or proceeding arising under subsection 1 and no such claim, action or proceeding shall be settled without the prior written approval of the Contractor and Canada.

3. If such a claim is made or appears likely to be made, Canada agrees to permit the Contractor to enable Canada at the Contractor's expense, to continue to use the equipment or software or to modify or replace it with equipment or software, which has published specifications equal or superior to the equipment or software being replaced. If the Contractor determines that none of these alternatives is reasonably available, Canada may elect, at the Contractor's expense, to independently secure the right to continue to use the equipment or software, or Canada may require the Contractor to accept the return of the equipment or software and to refund all monies paid to the Contractor under the Contract for the equipment and software, as well as all amounts paid for services and license and development fees.

4. The provisions of subsections 1 and 2 do not apply in situations where the Contractor was instructed by Canada to purchase a specific item of equipment or software from a specific source on behalf of Canada. In this case, the Contractor shall ensure that its subcontract for the equipment or software states that "If a third party claims that equipment or software that the subcontractor supplies under the Contract infringes any intellectual property right, the subcontractor, if requested to do so by either the Contractor or Canada, will defend the Contractor and Canada against that claim at the subcontractor's expense and will pay all costs, damages and legal fees that a court finally awards." In the event that the Contractor is unable to incorporate this into its subcontract, then it shall advise Canada of the situation and not proceed with the subcontract without receiving written notice from Canada that the level of intellectual property right infringement protection is acceptable.

5. Without prejudice to Canada's right to terminate the Contract for default prior to completion of the work, the above represents the Contractor's entire obligation to Canada regarding any claim of infringement.

6. The Contractor has no obligation regarding any claim based on any of the following:

   a. Canada's unauthorized modification of the equipment or software, or Canada's unauthorized use of the equipment or software in other than its published specified operating environment;

b. the combination, operation or use of the equipment or software with any product, data or apparatus that the Contractor did not provide under the Contract, or which combination, operation or use the Contractor did not authorize or approve in advance, if infringement would not have occurred but for such combination, operation or use."

7.37 Procurement Ombudsman

The parties understand that the Procurement Ombudsman appointed pursuant to Subsection 22.1 (I) of the Department of Public Works and Government Services Act will, on request and consent of the parties, participate in these meetings to resolve any such dispute, and subject to their consent to bear the cost of such process, provide to the parties a proposal for an alternative dispute resolution process to resolve their dispute. The Office of the Procurement Ombudsman may be contacted by telephone at 1-866-734-5169 or by e-mail at boa.opo@boa.opo.gc.ca.

7.38 Contract Administration

The parties understand that the Procurement Ombudsman appointed pursuant to Subsection 22.1 (I) of the Department of Public Works and Government Services Act will review a complaint filed by [the supplier or the contractor or the name the entity awarded the contract] respecting administration of the contract if the requirements of Subsection 22.2(1) of the Department of Public Works and Government Services Act and Sections 15 and 16 of the Procurement Ombudsman Regulations have been met, and the interpretation and application of the terms and conditions and the scope of the work of the contract are not in dispute. The Office of the Procurement Ombudsman may be contacted by telephone at 1-866-734-5169 or by e-mail at boa.opo@boa.opo.gc.ca.

Annexes

The following Annexes apply to and form part of the Contract:

ANNEX A: STATEMENT OF REQUIREMENTS

ANNEX B: BASIS OF PAYMENT

ANNEX C: SECURITY REQUIREMENTS CHECKLIST (SRCL)

Annex A - Statement of Requirements

Emergency Mass Notification Software Solution (EMNSS)

Objective

The Security and Internal Affairs Directorate, Finance and Administration Branch requires an Emergency Mass Notification Software Solution (EMNSS) that will allow for an efficient and consistent method of communicating with the 47000 employees of the Canada Revenue Agency (CRA) located in 99 buildings across the country before, during and after an emergency event.

Background

In the last couple of years, climate change has resulted in an increase to emergency weather related events in areas of Canada that were not normally exposed to such conditions. These events have identified a gap with current communication methods such as their call-trees or via the Building Status Line (BSL) a toll free telephone service, prompting Treasury Board of Canada Secretariat (TBS) to provide direction on what all departments need to communicate to their employees.

Not all emergency events result in building closures however, there is often other relevant information during an emergency event that must be shared with employees. As the BSL was designed with requirements to support only office closures, it cannot adequately support the current need and presents a gap in communicating with employees, especially after working hours.

Scope of requirement

CRA requires an EMNSS to broadcast notifications of threats or Emergency/Business Continuity Events. The following is a list of mandatory requirements:

ID	Mandatory Requirement Description
M1	The EMNSS proposed to meet this requirement must be off-the-shelf, meaning that each component of the EMNSS is commercially available and requires no further research and development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment).
M2	The provider must have delivered an EMNSS as a hosted application for at least three years.
M3	Service Design: The EMNSS must be designed specifically for emergency notifications with the capability of broadcasting mass notifications to multiple users within 15 minutes.
M4	Call Throttling: The EMNSS must have the ability to control the number of calls into an organization to avoid flooding the lines during a mass notification.
M5	Proprietorship: All hardware, software and data (apart from client's owned systems) must be hosted at facilities owned or leased, operated and secured in Canada.
M6	Platform: The EMNSS must not require the use of plug-ins for any functionality.
M7	The client must not be required to install any hardware or software to operate any facets of the EMNSS. Database capacity, data channels and phone ports are not purchased by the client.
M8	HotLine: The EMNSS must be able to transfer the current CRA Building Status toll free phone number to their system.
M9	Encryption: The Bidder must employ Communications Security Establishment Canada (CSEC) https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111 approved cryptography to protect sensitive data. The EMNSS user credentials for web console access (if equipped) must be encrypted in transit using the Transport Layer Security (TLS) version 1.2 or above.
M10	The EMNSS must provide mechanisms to protect the authenticity of communications sessions.
M11	The EMNSS must protect the confidentiality and integrity of information at rest.

ID	Mandatory Requirement Description
M12	The EMNSS must provide a facility for CRA to define role-based access to the data and functions of the EMNSS.
M13	Access Privileges: The EMNSS must enable Administrators to control access privileges, such as access requests, requests for changes to personal information, and changes to passwords, provided that they have appropriate access control permissions.
M14	Password Change: The EMNSS must permit each Administrator and user to change their password at any time.
M15	Password Strength: The EMNSS must force each Administrator and user to configure a password in a predetermined manner with a minimum number of characters, including capitals, numbers and symbols.
M16	The EMNSS must use replay-resistant authentication mechanisms for access to the system.
M17	The EMNSS must obscure feedback of authentication information during the authentication process.
M18	The EMNSS must allow Administrators to define and enforce a limit of invalid authentication attempts within a given time period. When the threshold has been met the information system locks the account until released by the administrator.
M19	Session Lock: The EMNSS initiates a session lock after an Administrator defined time period of inactivity. The information system retains the session lock until the user re-establishes access by re-authenticating.
M20	The EMNSS must protect against or limits the effects of denial of service attacks.
M21	The EMNSS must protect the integrity of transmitted information based on the CSEC approved communication algorithms https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111.
M22	Malicious Code Protection: The EMNSS must employ malicious code protections at all system entry and exit points, at workstations, servers, and/or mobile computing devices on the network to detect and eradicate malicious code on the system. The code protections (including signature definitions) should be updated whenever new releases are available. Regular scans of the information system are conducted daily and real-time scans are performed as files are downloaded, opened or executed in order to ensure that malicious code is detected, eradicated, and quarantined.
M23	The EMNSS must audit the following events: i. System Administrator access to the application ii. General user access to the application iii. Database maintenance activities iv. Application configuration changes
M24	The audit records produced by the EMNSS must contain sufficient information to: i. Identify the type of event that occurred ii. The date and time at which the event occurred iii. Where the event occurred iv. The source of the event v. The outcome of the event
M25	The EMNSS must ensure that sufficient storage capacity is available to prevent loss of audit records due lack of capacity. When maximum storage capacity of audit records has been reached the Bidder will notify the CRA administrator. The audit logs must be kept for a period of two years.
M26	The EMNSS must use internal system clocks to generate timestamps for audit records and that underlying servers use an authoritative time source (such as an Network Time Protocol (NTP) http://www.ntp.org/) to synchronize their clocks weekly.
M27	The EMNSS must ensure that access to audit records can be limited based upon the role based access permissions (for example, Administrators can view but not create, modify, or delete audit records while other users do not have access to the audit records).
M28	The EMNSS must protect audit records and ensures that audit information is backed up and retained for a period of two years.
M29	Users information records must be purged from the system immediately after the user unsubscribes from the system (i.e. no second copies of data are to be stored unless known to and authorized by the CRA). Purged data must not be recoverable.

ID	Mandatory Requirement Description
M30	The Administrators must have the ability to delete all transitory records.
M31	At the conclusion of the contract and/or at the request of the CRA, all CRA related information must be removed, and securely deleted from the EMNSS. The secure destruction of the data must be conducted in such a manner that no recovery can be performed. A letter of certification must be provided confirming destruction of all CRA data.
M32	Recovery: Client data must be hosted in high-availability facilities with zero fail-over time and automatic recovery.
M33	Disaster Recovery: If a disaster, emergency or hazard renders the EMNSS primary data centre inoperable, client data must be dynamically rerouted so that it functions without interruption.
M34	Back-Up Facilities and Services: The EMNSS must have a multi-tier, multi-server fault tolerant architecture with full redundancy whereby the users contact information database server and all EMNSS functions are housed in Canada and their back-up capability is housed in separate locations in Canada separated by a provincial boundary (at least 200 km) so that an emergency that affects one facility will not affect the others.
M35	Location of Data Servers: The EMNSS must ensure that the client's database never resides outside of Canada's land boundaries.
M36	Permissions and Access Controls: The EMNSS must enable and support the designation of a minimum of 10 Master Administrators with full access, Regional and Local (building) Administrators with limited access.
M37	User Interfaces: The EMNSS must provide graphical user interfaces (GUI) in both English and French for all users.
M38	Browsers: The EMNSS must be accessible to Administrators and users on web browsers including Internet Explorer (min version 9.0), Microsoft Edge, Apple Safari (min version 5.1), Google Chrome (min version 17.0) and Mozilla Firefox (min version 10.0) for Windows - and compatible with 128-bit encryption.
M39	Quick Launch: The EMNSS must have a quick-launch feature that allows an Administrator to initiate a message from a single screen after logging in to the EMNSS.
M40	Practice Modes: The EMNSS must have practice modes (i.e., a test environment) that allow the Administrators to use any facet of the EMNSS without affecting real-time content or capabilities of the EMNSS and the database (i.e., the production environment).
M41	Self-Registration: The EMNSS must allow to self-register and update their own profile information at any time.
M42	Mapping: The EMNSS must have a map function to select a radius surrounding an event for notifications to be sent to only the selected geographic area.
M43	Voice Messages: The EMNSS must send local or long-distance voice messages of up to 1 minute in duration (exclusive of dialing time, ringing time and voice-mail response time).
M44	Voice Message Language: Voice messages must be delivered with voices using Canadian English and Canadian French.
M45	Text-based Messages: The EMNSS must send text-based SMS messages of a minimum of 140 characters or e-mail messages of up to 500 words to at least 13000 registered users within 10 minutes of being sent.
M46	Reliability: The EMNSS must be fully functional and operational 24 hours a day, 7 days a week, with at least 99.99% availability throughout the Contract period. In the event of an outage, the EMNSS provider will advise the client within 30 minutes of the outage and the impacts on the EMNSS.
M47	Reliability: In the event of a scheduled outage, the Bidder will advise the client at least 5 business days in advance of the outage.
M48	Support: The EMNSS must offer technical support 24 hours a day, 7 days a week.
M49	Native SMS in Canada: The EMNSS must use short code (5 digits number) in order to allow for the sending of true SMS versus email-to-SMS.
M50	Data Recovery: The EMNSS must enable Administrators to recover a user contact record that has been deleted for up to 5 days after deletion.
M51	Database Backup: The EMNSS must generate automatic database backups to one or more other locations in Canada at least once every 24 hours.
User Information	

M52	Administrator and User Profiles: The EMNSS must allow for the establishment and maintenance of a database of Administrator and user profiles that include the following:
	i. Full name
	ii. Region
	iii. Branch
	iv. Business address
	v. Home address
	vi. Cell phone number
	vii. Home phone number
	viii. Business phone number
	ix. Personal e-mail address
	x. Work e-email address
	xi. Designated alternate
	xii. Permissions assigned
	xiii. Master Administrators must have full access permissions to perform all functions of the EMNSS.
M53	User Information Data Fields: The EMNSS must enable Administrators to identify mandatory data fields.
M54	User Information Data Fields: The EMNSS must accommodate the creation of 25 data fields per record.
M55	Data Revision: The EMNSS must enable Administrators and users to view and manually edit the information in their own profiles, directly within the EMNSS, provided they have appropriate access control permissions.
M56	Data Revision: The EMNSS must enable Administrators and users to add, modify, and delete user information, directly within the EMNSS, provided they have appropriate access control permissions.
Groups	
M57	Creation: The EMNSS must enable Administrators to create groups based on variables such as Region, Building or other criteria identified in the data fields of each user's record.
M58	Hierarchical Groups: The EMNSS must enable Administrators to create hierarchical groupings so that groups include up to 30 levels of sub-groups in order to appropriately reflect an organization's structure.
M59	Number of Groups: The EMNSS must enable Administrators and users to define a user to be a member of up to 50 groups.
Message initiation	
M60	Service Access: The EMNSS must enable Administrators to access the service for user management, message creation (voice or text-based) or message transmission purposes via the following methods and devices:
	i. Computer (via the internet either through cable or WI-FI or Voice over Internet protocol);
	ii. Landline telephone;
	iii. Cellular telephone;
	iv. Teletype device (TTY); and
	v. EMNSS Application.
M61	Message Creation: The EMNSS must enable Administrators to create and save templates in French and English.
M62	Message verification: Administrators must be able to hear the voice message and/or to read the text-based message before it is sent. Administrators must be able to edit or rerecord the message if it was not correct.
M63	Time Zone Recognition: The EMNSS must recognize and process to the relevant time zones for notifications that are sent from a time zone, but delivered to another time zone.
Message transmission	
M64	Media: The EMNSS must send messages to users via the following:
	i. Landline telephone;
	ii. Cellular telephone;
	iii. SMS text message;
	iv. E-mail;
	v. Teletype device (TTY); and
	vi. EMNSS Mobile Application (push notifications).
M65	Safeguards: The EMNSS must have an effective safeguard (such as a prompt message) that prevents routine messages from being sent out as emergency notifications.
M66	Phone Number Types: The EMNSS must have the ability to make local and long distance calls within Canada.

M67	Order of Contact Methods: The EMNSS must enable Administrators and users to set the default order of devices used to notify users.
M68	Language of Message: The EMNSS must enable Administrators to create messages in French and English and to automatically transmit them in the user's pre-selected corresponding language.
M69	Simultaneous Transmission: Administrators must be able to send a recorded voice message and a text message in a single notification to all selected users for delivery through the media listed in **M64**.
M70	Caller ID: Either globally or on a message-by-message basis, the EMNSS must enable Administrators initiating a message to customize the telephone number displayed (caller ID) for voice messages and the e-mail addresses for text-based messages.
M71	Escalation: The EMNSS must escalate messages when the intended user has not confirmed receipt of the correspondence (with 3 levels of escalation) within a given period of time.
M72	Delivery Attempts: Administrators must be able to select the number of delivery attempts through all contact method paths.
M73	E-mail Attachments: The EMNSS must be able to attach multiple files (e.g. text, spreadsheet and images) to e-mails.
M74	Message Control: Administrators must be able to stop, recall or replace a message initiated by them or another Administrator with the same or higher level of permissions at any time during the message sending process.
M75	Designated alternate: The EMNSS must automatically send messages to a designated alternate (if one has been designated) if a user does not acknowledge receipt of the initial message within a period of time defined by the sender.
M76	First to Respond: The EMNSS must have the capability to send notifications systematically until a predetermined number of affirmative responses are received.
M77	Roll Call: The EMNSS must have the capability to send notifications for the purpose of soliciting an acknowledgement from the recipient..
M78	HotLine: When calling the EMNSS hotline, users must only obtain notifications pertaining to the individual work site(s) they have registered for (physical building location). Users are not to obtain or have to listen to any notifications for other work sites they have not registered for.
Message delivery features	
M79	Voice Message Repeat: The EMNSS must allow the users to listen to a voice message as often as desired with a single key press.
M80	Voice-Mail: The EMNSS must leave a message when a voice-delivered message reaches an answering machine or voicemail. If a message is left, the EMNSS must also contact the next contact method if the message was left on the primary contact method.
Message management	
M81	Scheduling: The EMNSS must enable Administrators to schedule a notification to be sent at a future date and time.
M82	Mass notifications: The EMNSS must have unlimited and unrestricted mass notifications capabilities.
Reporting	
M83	Dashboard: The EMNSS must provide a real-time dashboard for each active notification broadcast allowing Administrators to view broadcast parameters (e.g. devices, start time, duration and number of cycles) and see status of broadcast results (e.g. delivery confirmation).
M84	History: The EMNSS must enable Administrators to view a history of message results for the entire period of the contract.
M85	Audit Trail: The EMNSS must produce real-time message broadcast result reports using all application data which contains, but is not limited to, all of the following information: i. Name, date and time of the message; ii. Name of the Administrator or user who initiated the broadcast; iii. Summary statistics, including total notified users, total confirming receipt/not confirming receipt, percentage confirming receipt/not confirming receipt. This information must be collated for individual messages and cumulatively; and iv. Detailed calling information, including call-result of each attempt within the broadcast, the addresses and associated phone numbers attempted, the attempt number and the result (e.g., confirmed with date and time, busy, no answer or voicemail).

M86	Export: The EMNSS must export all types of report data in CSV, XLS, HTML, or PDF formats, as defined by an Administrator or user.
M87	Printing: The EMNSS must enable Administrators to print real-time reports of any data or statistics directly from the GUI.
M88	Reports: Upon request, the Bidder must search and generate reports based on user-defined criteria and/or key words including wild card searches. In addition, the Bidder must retain, on their servers, a record of all reports for the entire period of the contract.
Training	
M89	The Bidder must provide in-house training on CRA premises.
M90	The EMNSS must be supplied with manuals downloadable from the Internet.
M91	The EMNSS manuals must define all functions and include complete instructions for the operation of the product.

Annex B – Basis of Payment

BASIS OF PAYMENT - FIRM REQUIREMENT

For fulfilling all of its obligations as specified under the Contract, the Contractor will be paid firm all inclusive prices for the goods and services as set out in Table 1 below. DDP, Customs duty is included, if applicable; and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable, in accordance with the Method of Payment and Invoicing clauses identified herein.

Table 1 – Firm Requirement						
Item No.	Description	Unit of Issue	Firm Price (excludes GST/HST)	Firm Price (excludes GST/HST)	Firm Price (excludes GST/HST)	Extended Price (excludes GST/HST)
			Year 1	Year 2	Year 3	
1	Emergency Mass Notification Software Solution (EMNSS)	Unlimited Users	$	$	$	$
2	Initial In-Class Room Training	Each	$	Not Applicable	Not Applicable	$
					Total	$

If the options identified below are exercised, the Contractor will be paid the firm prices for the goods and services as set out in Tables 2 - 3. DDP, Customs duty is included, if applicable; and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable, in accordance with the Method of Payment and Invoicing clauses identified herein.

Table 2 – Optional Additional Years									
Item No.	Description	Unit of Issue	Firm Price (excludes GST/HST)	Firm Price (excludes GST/HST)	Firm Price (excludes GST/HST)	Firm Price (excludes GST/HST)	Firm Price (excludes GST/HST)	Firm Price (excludes GST/HST)	Firm Price (excludes GST/HST)
			Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
1	Emergency Mass Notification Software Solution (EMNSS)	Unlimited Users	$	$	$	$	$	$	$

Table 3 – Optional Training			
Item No.	Description	Unit of Issue	Firm Price (excludes GST/HST)
1	In-Class Room Training	Each	$

Annex C – Security Requirements Check List (SRCL)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
1000348508
Security Classification / Classification de sécurité

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine — Canada Revenue Agency

2. Branch or Directorate / Direction générale ou Direction — FAB / SIAD

3. a) Subcontract Number / Numéro du contrat de sous-traitance

3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

CRA requires the Emergency Mass Notification System to quickly alert its employees before, during and after an emergency situation.

5. a) Will the supplier require access to Controlled Goods?
Le fournisseur aura-t-il accès à des marchandises contrôlées? — [✓] No / Non [ ] Yes / Oui

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

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?
Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?
(Specify the level of access using the chart in Question 7. c)
(Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) — [ ] No / Non [✓] Yes / Oui

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted.
Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. — [✓] No / Non [ ] Yes / Oui

6. c) Is this a commercial courier or delivery requirement with no overnight storage?
S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit? — [✓] No / Non [ ] Yes / Oui

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

Canada	[✓]	NATO / OTAN	[ ]	Foreign / Étranger	[ ]

7. b) Release restrictions / Restrictions relatives à la diffusion

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

7. c) Level of information / Niveau d'information

Canada		NATO		Foreign / Étranger	
PROTECTED A / PROTÉGÉ A	[✓]	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	[ ]	PROTECTED A / PROTÉGÉ A	[ ]
PROTECTED B / PROTÉGÉ B	[ ]	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	[ ]	PROTECTED B / PROTÉGÉ B	[ ]
PROTECTED C / PROTÉGÉ C	[ ]	NATO CONFIDENTIAL / NATO CONFIDENTIEL	[ ]	PROTECTED C / PROTÉGÉ C	[ ]
CONFIDENTIAL / CONFIDENTIEL	[ ]	NATO SECRET / NATO SECRET	[ ]	CONFIDENTIAL / CONFIDENTIEL	[ ]
SECRET / SECRET	[ ]	COSMIC TOP SECRET / COSMIC TRÈS SECRET	[ ]	SECRET / SECRET	[ ]
TOP SECRET / TRÈS SECRET	[ ]			TOP SECRET / TRÈS SECRET	[ ]
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	[ ]			TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	[ ]

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Government of Canada Gouvernement du Canada	Contract Number / Numéro du contrat
	1000348508
	Security Classification / Classification de sécurité

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

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

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

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

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

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

☑ RELIABILITY STATUS / COTE DE FIABILITÉ   ☐ CONFIDENTIAL / CONFIDENTIEL   ☐ SECRET / SECRET   ☐ TOP SECRET / TRÈS SECRET

☐ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT   ☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL   ☐ NATO SECRET / NATO SECRET   ☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET

☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS

Special comments:
Commentaires spéciaux : _____

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

10. b) May unscreened personnel be used for portions of the work?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?   ☑ No / Non   ☐ Yes / Oui

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

TBS/SCT 350-103(2004/12) | Security Classification / Classification de sécurité | Canada

Government of Canada — Gouvernement du Canada

Contract Number / Numéro du contrat
1000348508
Security Classification / Classification de sécurité

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

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.

Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?   ✓ No / Non   ☐ Yes / Oui

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

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?   ✓ No / Non   ☐ Yes / Oui

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

TBS/SCT 350-103(2004/12)   Security Classification / Classification de sécurité   Canada

	Government of Canada	Gouvernement du Canada	Contract Number / Numéro du contrat
			1000348508 \
			Security Classification / Classification de sécurité

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Debby Honcoop	Director	*Honcoop*

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-943-8925	613-943-9215	Debby.Honcoop@cra-arc.gc.ca	Sept 25, 2019

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
LAN PHUNG	CORPORATE SECURITY	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613 957-7488			Sept 25, 2019

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

☐ No / Non   ☑ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

RECEIVED / REÇU

SEP 2 5 2019

Security Directorate
Direction de la Sécurité

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canadä

Information Security Requirements

The Contractor must abide by the following Information Security Requirements:

- Access to CRA Protected information and systems containing CRA Protected information is to be provided to appropriately cleared personnel and on a need to know basis only;
- Protected A information can be stored on cloud based systems providing the Contractor demonstrates their ability to protect data in accordance with the Document safeguarding capabilities (DSC) for Protected A.
- Use of standalone dedicated equipment (such as laptop) is required to store and perform work on CRA Protected information;
- Equipment handling CRA Protected information is to be fully encrypted (MS BitLocker is the CRA standard to fully encrypt hard drive of the standalone equipment);
- Equipment must be built with appropriate anti-virus, anti-malware, anti-spyware, etc. security safeguards;
- Equipment handling CRA Protected information must be set with access control (as a minimum UserID and Password are to be used);
- Screen savers are to pop-up after 10 to 15 minutes of session inactivity and requires passwords to continue the session;
- CRA Protected information must be stored on encrypted PDSD:
  - USB devices
    - MS BitLockerToGo (BTG) is the CRA standard to encrypt USB devices;
  - CD devices
    - McAfee File and Removable Media Protection is one of the CRA standard to encrypt CD devices or;
    - WinZip is the other CRA standard to encrypt CD devices;
- PDSDs may not contain a mixed of CRA and Non-CRA data;
- Protected information sent via email is to be contained in encrypted attachments (WinZip is one of CRA standard to encrypt attachments – see below for additional security rules for using WinZip);
- All CRA Protected information is to be deleted/destroyed at the end of the contract (Hard drives requires to be wiped, Portable Data Storage Devices (PDSD) such as USB/CD, must be sent back to CRA, paper documents are to be shredded).

Additional security rules for sending zipped (WinZip) files via email:

- The email's subject line must never contain any Protected information;
- Protected data must not be in the body text (description) of the email but within attached Zipped and Encrypted documents (in MS Word, Excel, or PowerPoint);
- The name of the Zipped file is not to contain any Protected information;
- The encryption method is to be set to 256-bit AES;
- Password must not be a word of the dictionary or a name;
- The minimum password length must be 8 characters long;
- The password must contain:
  - at least one lower case character (a-z),
  - at least one upper character (A-Z),
  - at least one numeric character (0-9), and
  - at least one symbol character (!, @, #, $, %, ^, &, …).
- The one time password must be provided either via the telephone or within a second email message but only sent after receiving confirmation of reception of the message containing the Zipped/Encrypted file;
- The email must be sent to one destination only (one email address).

Additional security rules for McAfee File and Removable Media Protection:

- To decrypt the CD, insert the encrypted CD/DVD into the optical drive. McAfee File and Removable Media Protection – Removable Media window will come up. If it does not automatically come up, navigate to the CD drive and run **MfeEERM.exe**

Physical Security Requirements

- The Outside Consultant are to store CRA protected information in a locked container located in a locked room when not in use;
- The Outside Consultant are to store CRA protected waste in a locked container until it is returned to CRA to be destroyed;
- The Outside Consultant must report immediately any actual or suspected loss, or unauthorized disclosure of information to CRA security official;
- The Outside Consultant must report immediately any theft of CRA asset (laptop) to the Agency Operations Centre (AOC) of the Security and Internal Affairs Directorate at 1-866-362-0192 and to the functional authority for the contract.

In Transit

- The Outside Consultant should as a general rule, exercise good judgment and ensure that every reasonable effort has been made to minimize the risk to CRA protected information or asset (laptop) at all times;
- The Outside Consultant are to secure CRA protected information and asset (laptop) in a locked briefcase when transporting the information. The briefcase must be tagged with a forwarding or return address and/or phone number of the Outside Consultants' office. While travelling by vehicle, the briefcase must be placed in a locked trunk, or out of sight in a locked vehicle;
- While on public transit systems, the Outside Consultant are to maintain control of the briefcase containing CRA protected information and are not to expose the material to others.