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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.,/11, rue Laurier
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

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

Issuing Office - Bureau de distribution

Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Title - Sujet National Cybercrime Solution Projec Solution nationale en matière de cybercriminalité	
Solicitation No. - N° de l'invitation M7594-205915/D	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client M7594-205915	**Date** 2021-04-12
GETS Reference No. - N° de référence de SEAG PW-$$XL-155-39352	
File No. - N° de dossier 155xl.M7594-205915	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-05-25 Heure Avancée de l'Est HAE

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à: Labossière, Jean-Claude	**Buyer Id - Id de l'acheteur** 155xl
Telephone No. - N° de téléphone (613) 858-7359 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Instructions: See Herein

Instructions: Voir aux présentes

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

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

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Canada

This amended final bid solicitation document cancels and supersedes the previously posted final bid solicitation document in its entirety.

BID SOLICITATION

NATIONAL CYBERCRIME SOLUTION FOR CANADA ROYAL CANADIAN MOUNTED POLICE

Table of Contents

BID SOLICITATION

NATIONAL CYBERCRIME SOLUTION

FOR
CANADA ROYAL CANADIAN MOUNTED POLICE

PART 1 – GENERAL INFORMATION

1.1 Introduction

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

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

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

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

Part 4 Evaluation and Assessment Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, the Capability and Usability Assessment to be conducted on the Prototype solution(s), and the basis of selection for full Solution implementation;

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

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

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

The annexes include the Statement of Work and any other annexes.

1.2 Summary

(a) A Request for Information (RFI) (M7594-200151/A) was issued on 2019/06/05. The main goal of the engagement with Industry was to solicit industry feedback on Canada's high-level requirements to determine industry's interest and capacity to provide the proposed Solution.

(b) Notices of Proposed Procurement (NPP) M7594-205915/A, M7594-205915/B and M7594-205915/C were respectively issued on 2020/05/22, 2020/12/03, and 2021/01/28 to further engage industry and to obtain industry feedback and comments on Canada's draft requirements and procurement approach in order to allow Canada better define its requirements and procurement approach.

(c) The current bid solicitation aims to procure the National Cybercrime Solution (NCS) (the "Solution") for the Royal Canadian Mounted Police (RCMP) (the "Client"). However, the bid solicitation will also allow Canada to make the Solution available to any department or Crown corporation (as those terms are defined in the Financial Administration Act) or any other party for which the Department of Public Works and Government Services is authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act (each a "Client"). Although Canada may make the Software Solution available to any or all the Clients, this bid solicitation does not preclude Canada from using another method of supply for entities of the Government of Canada with the same or similar needs.

(d) The bid solicitation is intended to result in the award of up to three Contracts to successful Bidders for Phase 1 work to each develop a Capability and Usability Assessment (CUA) Prototype Solution in accordance with Phase 1 of Annex A –Statement of Work. On completion of Phase 1 work and on assessment of the Prototype solutions by Canada, and successful completion of a Prototype on Platform (PoP) Test by a Contractor (if applicable), Canada will at its sole discretion exercise the option for the Contractor to deliver the full Solution in accordance with Phase 2 of Annex A – Statement of Work. Following the Phase 2 Full Solution implementation Work, Canada will, at its sole discretion, exercises 8 one-year irrevocable option periods to extend the term of the resulting Contract(s) as and when required.

(e) While Canada intends to issue Contract(s) of a specific duration, Canada reserves the right to continue to Contract for and leverage this Solution for as long as it makes business sense for Canada to do so. Canada also expects that this type of Solution will evolve with time and technology, including incorporation of functionalities or technologies that isn't currently part of the requirement. Canada reserves the right to consider these evolutionary functionalities or technologies to be part of the ongoing scope of the work being done under the Contract, subject to Canada's internal approval processes. Canada reserves the right to, at a subsequent date and at its sole discretion, identify the solution either as a multi-departmental solution, or designate the solution as a Government of Canada (GC) Enterprise-wide standard if and when determined by the GC-Enterprise Architecture Review Board (GCEARB).

(f) The Client is seeking a Solution delivered via a Cloud Service Delivery Model that may be comprised of any combination of Software hosted by the RCMP, on the RCMP Protected B Cloud Tenant Infrastructure as a Service (IaaS), Private Platform as a Service (PaaS), Public Platform as a Service (PaaS) and Software as a Service (SaaS) using a Government of Canada approved Protected B Cloud Service platform. The required Solution may be comprised of any combination of commercial-off-the-shelf ("COTS"), open source or custom software; the resulting configuration of such software must allow operation of the Solution at all times in accordance with Annex A – Statement of Work. The Contractor must define a Cloud Service Delivery Model that is compatible with Government of Canada (GC) Cloud Services Protected B security requirements.

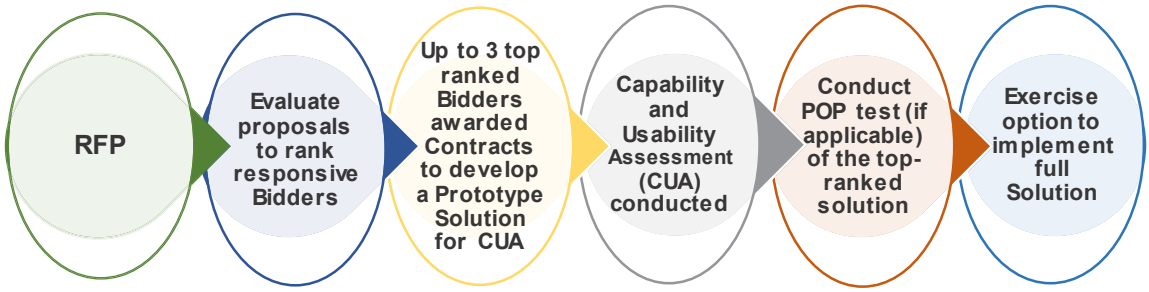
(g) The scope of work for the CUA Prototype Solution includes the planning, design, development, configuration, testing, and delivery of a production quality, hosted, Cloud based, working Minimum Viable Product (MVP) solution supporting up to one-hundred (100) Users in accordance with the required technical and functional requirements described in Annex A – Statement of Work.

(h) The scope of work for the Full Solution includes the planning, design, development, configuration, documentation, testing and deployment of all functional and non-functional capabilities as described in Appendix C – NCS Business Capability Model of Annex A – Statement of Work. The Solution must support up to 2000 users, including 500 concurrently,

and be capable of supporting processes and analysis activities that are estimated to accumulate 110TB of data per year. See Annex A – Statement of Work for details.

(i) The bid solicitation and the resulting Contract(s) will follow an agile procurement approach in order to encourage more effective collaboration with vendors. Being agile means approaching the project in short phases while assessing and addressing challenges along the way.

(j) The anticipated multi-phase agile procurement process will be conducted as per the following phases:



1.3 Overview of the Project

(a) The Government of Canada is seeking a Software Solution that will be deployed in a Protected B, Medium Integrity, Medium Availability (PBMM) cloud-based solution tenant**.** The required Solution may be comprised of any combination of commercial-off-the-shelf ("COTS"), open source or custom software; the resulting configuration of such software must allow operation of the Solution at all times in accordance with Annex A – Statement of Work. . The Contractor will configure the Solution such that it:

1. meets Government of Canada security requirements and industry best practices;
2. includes secure maintenance and technical support;
3. includes training and other professional services as and when requested; and
4. includes regularly updated English and French training materials and solution documentation including all requisite software licenses and warranties.

The Government of Canada will retain ownership of all data in the solution including business data, monitoring data, and metadata.

(b) The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the Canada-Chile Free Trade Agreement (CCFTA), the Canada-Columbia Free Trade Agreement (CCFTA), the Canada-Panama Free Trade Agreement (CPFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA) if it is in force, the Canadian Free Trade Agreement (CFTA), Canada-Honduras Free Trade Agreement (CHFTA), Canada-Korea Free Trade Agreement (CKFTA), Canada-Peru Free Trade Agreement (CPFTA), Canada-Ukraine Free Trade Agreement (CUFTA), and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).

(c) The bid solicitation will allow bidders to use the epost Connect service provided by Canada Post Corporation to transmit their bid electronically. Bidders must refer to Part 2 entitled Bidder Instructions, and Part 3 entitled Bid Preparation Instructions, of the bid solicitation, for further information.

(d) "The Federal Contractors Program (FCP) for employment equity applies to this procurement: refer to Part 5 – Certifications and Additional Information, Part 7 – Resulting Contract Clauses and the form titled Federal Contractors Program for Employment Equity – Certification."

Overview of the Agile Procurement Approach

The procurement process will be conducted using an agile approach as follows:

1) **Bid Solicitation (Phase 1):** This bid solicitation is issued through the Government Electronic Tendering Service for a defined solicitation period to satisfy the requirements of the **Client.** The bid solicitation document is available to all Bidders. Bidders have the opportunity to review the bid solicitation document, to seek clarification on any aspect of the bid solicitation document and to submit a bid in response to the bid solicitation.

2) **Evaluate proposals to determine and rank responsive Bidder(s) (Phase 2)**: Bids will be assessed in accordance with all requirements of the bid solicitation. Bids will be evaluated based on the Technical and Financial evaluation criteria identified in the bid solicitation. Bidders meeting all the mandatory requirements of the bid solicitation will be ranked based on the highest combined rating of the technical and financial evaluations. The detailed evaluation process is described in Part 4 – Evaluation and Assessment Procedures and Basis of Selection.

3) **Award Contracts to up to 3 top ranked Bidders to deliver a Prototype Solution (Phase 3)**: Based on the results of the Technical and Financial evaluation, Canada may award up to 3 Contracts each initially valued at $200,000 (GST/HST extra), to the 3 top ranked Bidders to develop and deliver a prototype Solution within a stipulated period in accordance with Phase 1 Work described in Annex A-Statement of Work and the Capability and Usability Assessment (CUA) criteria in Appendix A to Annex A-Statement of Work.

4) **Conduct Capability and Usability Assessment (CUA) (Phase 4)**: Upon completion and delivery of all required deliverables, including the Prototype Solution for Phase 1 Work in Annex A-Statement of Work, Canada will conduct a CUA assessment in accordance with the CUA criteria in Appendix A to Annex A-Statement of Work. The detailed CUA assessment process is described in Part 4 – Evaluation and Assessment Procedures and Basis of Selection.

5) **Conduct POP Test of the CUA top-ranked solution (Phase 5)**: Following the conduct of the CUA assessment, the Contractors will be ranked based on the highest combined rating of their technical, financial and CUA scores. A Prototype on Platform (POP) Test may be conducted, at Canada's sole discretion, on the solution proposed by the top-ranked Contractor (identified after the CUA) to validate technical and functional requirements. The detailed PoP test process is described in Part 4 – Evaluation and Assessment Procedures and Basis of Selection.

6) **Exercise option to implement full Solution (Phase 6)**: Canada will, at its sole discretion, exercise its irrevocable option in favour of the highest ranked contractor whose prototype solution has been validated against the technical and functional requirements of the NCS. The exercise of this option will initiate the implementation of the full Solution in accordance with Phase 2 Work described in Annex A- Statement of Work. It is Canada's intent to exercise

its irrevocable option to the top ranked Contractor to implement the full Solution. However, Canada may at its sole discretion exercise its irrevocable option on the other Contract(s) for a portion of the Work described for Phase 2 in Annex A-Statement of Work if it is determined that this would best meet the needs of Canada.

1.4 Security Requirements

(a) There are security requirements associated with this procurement. Different security requirements will apply to each of the resulting Phase 1 Work and Phase 2 Work described in the Annex A- Statement of Work. Before award of a contract for Phase 1, and before extending a contract for Phase 2, the following conditions must be met:

(i) the Bidder/Contractor must hold a valid organization security clearance as indicated in Part 6 – Resulting Contract Clauses;

(ii) the Bidder/Contractor's proposed individuals requiring access to classified or protected information, assets or sensitive work sites must meet the security requirements as indicated in Part 6 – Resulting Contract Clauses;

(iii) the Bidder/Contractors must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites;

(iv) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 6 – Resulting Contract Clauses; and

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

(b) Bidders/Contractors are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder/Contractor to obtain the required clearance will be at the entire discretion of the Contracting Authority.

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

1.5 Debriefings

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

1.6 Conflict of Interest – Unfair Advantage

(a) In order to protect the integrity of the procurement process, Bidders are advised that Canada may reject a bid in the following circumstances:

(i) if the Bidder, any of its subcontractors, any of their respective employees or former employees was involved in any manner in the preparation of the bid solicitation or in any situation of conflict of interest or appearance of conflict of interest;

(ii) if the Bidder, any of its subcontractors, any of their respective employees or former employees had access to information related to the bid solicitation that was not available

to other Bidders and that would, in Canada's opinion, give or appear to give the Bidder an unfair advantage.

(b) The experience acquired by a bidder who is providing or has provided the goods and services described in the bid solicitation (or similar goods or services) will not, in itself, be considered by Canada as conferring an unfair advantage or creating a conflict of interest. This bidder remains however subject to the criteria established above.

(c) Where Canada intends to reject a bid under this section, the Contracting Authority will inform the Bidder and provide the Bidder an opportunity to make representations before making a final decision. Bidders who are in doubt about a particular situation should contact the Contracting Authority before bid closing. By submitting a bid, the Bidder represents that it does not consider itself to be in conflict of interest nor to have an unfair advantage. The Bidder acknowledges that it is within Canada's sole discretion to determine whether a conflict of interest, unfair advantage or an appearance of conflict of interest or unfair advantage exists.

(d) Without limiting in any way the provisions described in 1.6(a) above, Bidders are advised that Canada has engaged the assistance of the following private sector contractor(s) and resource(s) who have provided services including the review of content in preparation of this bid solicitation document and/or who have had, or may have had, access to information related to the content of this or other documents related to this solicitation:

ADGA Group Consultants Inc.
• Joe Carlucci
• Gardy Joseph

Cache Computer Consulting Corp
• Todd Mennie

Cofomo Ottawa (formerly operating as: Emerion)
• Ying Chen
• John Zhang

Experis-Veritaaq
• Justin Richardson
• Kevin Yang
• David Dang

Gartner, Inc.
• Chris Litton
• Alasdair Maughan
• Corry Robinson

Info-Tech Research Group
• Alex Ciraco

MODIS
• Joan Duval
• Patrick Quinlan
• Deborah Rudd
• Alex Aronec

S.i. Systems ULC

- Warren Chen
- Richard Legault
- Brad Martel
- Rob Webb
- Scott Webster
- Andrew Taylor

The Powell Group-TPG Technology Consulting Ltd
- Stephen Archdeacon

(e) Any bid that is received from one of the above-noted contractors in 1.6(d), whether as a sole Bidder, joint venture or as a sub-contractor to a Bidder; or for which one of the above-noted resources provided any input into the bid, will be considered to be in contravention of the Conflict of Interest clauses identified in this section, and the bid will be declared non-responsive.

1.7 Phased Bid Compliance Process

The Phased Bid Compliance Process applies to this requirement as described in Part 4 – Evaluation and Assessment Procedures and Basis of Selection.

PART 2 – BIDDER'S INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

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

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

(c) The 2003 (2020-05-28) Standard Instructions – Goods or Services – Competitive Requirements, are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003 and this document, this document prevails.

(d) Subsection 5(4) of 2003, Standard Instructions – Goods or Services – Competitive Requirements is amended as follows:

(i) Delete: 60 days
(ii) Insert: 180 days

(e) The 2003, Standard Instructions is amended as follows:

1. Section 5, entitled Submission of bids, is amended as follows:

(i) subsection 1 is deleted entirely and replaced with the following: "Canada requires that each bid, at solicitation closing date and time or upon request from the Contracting Authority, for example in the case of epost Connect service, be signed by the Bidder or by an authorized representative of the Bidder. If a bid is submitted by a joint venture, it must be in accordance with the section entitled Joint venture."

(ii) subsection 2.d is deleted entirely and replaced with the following: "send its bid electronically only to the specified Bid Receiving Unit of Public Services and Procurement Canada (PSPC) identified in the bid solicitation; or to the address specified in the bid solicitation, as applicable;"

(iii) subsection 2.e is deleted entirely and replaced with the following: "ensure that the Bidder's name, return address and procurement business number, bid solicitation number, and solicitation closing date and time are clearly visible on the bid; and,"

2. Section 6, entitled Late bids, is deleted entirely and replaced with the following: "PSPC will return bids delivered after the stipulated solicitation closing date and time, unless they qualify as a delayed bid as described in the section entitled Delayed bids. For bids submitted using means other than the Canada Post Corporation's epost Connect service, the bid will be returned. For bids submitted using Canada Post Corporation's epost Connect service, conversations initiated by the Bid Receiving Unit via the epost Connect service that contain access, records and information pertaining to a late bid will be deleted."

3. Section 07, entitled Delayed bids, is amended as follows: Subsection 1 is amended to add the following piece of evidence: "d. a Canada Post Corporation's epost Connect service date and time record indicated in the epost Connect conversation activity."

4. Section 8, entitled Transmission by facsimile, is deleted and replaced by the following:

"by epost Connect"

2.2 Submission of Bids

(a) Bids must be submitted on or before the closing date and time indicated on page 1 of the bid solicitation by Canada Post Corporation's epost Connect at Public Services and Procurement Canada (PSPC) Bid Receiving Unit email address: tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca .

(b) Due to the nature of the bid solicitation, bids transmitted by facsimile to PWGSC will not be accepted.

2.3 Former Public Servant (FPS)

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

Definitions

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

(a) an individual;

(b) an individual who has incorporated;

(c) a partnership made of former public servants; or

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

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

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

11, the *Members of Parliament Retiring Allowances Act*, R.S. 1985, c. M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, c. C-8.

Former Public Servant in Receipt of a Pension

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

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

(a) name of former public servant;

(b) date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

Work Force Adjustment Directive

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

If so, the Bidder must provide the following information:

(a) name of former public servant;

(b) conditions of the lump sum payment incentive;

(c) date of termination of employment;

(d) amount of lump sum payment;

(e) rate of pay on which lump sum payment is based;

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

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

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes.

2.4 Enquiries – Bid Solicitation

(a) All enquiries must be submitted in writing to the Contracting Authority no later than 5 calendar days before the bid closing date. Enquiries received after that time may not be answered.

(b) Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that

the Bidder do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered with copies to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 Applicable Laws

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

> ***Note to Bidders:*** Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidder. *Bidders are requested to indicate the Canadian province or territory they wish to apply to any resulting contract in their Bid Submission Form*.

2.6 Improvement of Requirement during Solicitation Period

Should Bidders consider that the specifications or Statement of Work and Statement of Requirements contained in the bid solicitation could be improved technically or technologically, Bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reasons for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority in accordance with the article entitled “Enquiries – Bid Solicitation”. Canada will have the right to accept or reject any or all suggestions.

2.7 Volumetric Data

The data provided in this bid solicitation has been provided to Bidders to assist them in preparing their bids. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage will be consistent with this data. It is provided purely for information purposes.

2.8 Bid Challenge and Recourse Mechanisms

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

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

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

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

PART 3 – BID PREPARATION INSTRUCTIONS

Bids are to be prepared in accordance with SACC 2003 Standard Instructions – Goods or Services – Competitive Requirements and the articles described here in Part 3 - Bid Preparation Instructions.

3.1 Bid Preparation Instructions

(a) The Bidder must submit its bid electronically, Canada requests that the Bidder submits its bid in accordance with section 08 of the SACC 2003 Standard Instructions – Goods or Services – Competitive Requirements. Bidders must provide their bid in a single epost Connect message. The Canada Post Corporation's epost Connect service has the capacity to receive multiple attached files per individual message. The maximum total size of an individual message is 1GB, including attachments. Should a bidder not have a Canadian mailing address, they may use the Bid Receiving Unit (BRU) email address <**tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca**> in order to register for the epost Connect service. Bids will not be accepted if emailed directly to this BRU email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to send bids through an epost Connect message if the bidder is using its own licensing agreement for epost Connect.

(b) The Bidder must present the following sections of their bid in one (1) PDF:

Section I: Technical Bid (all content, excluding other file types)

Section II: Financial Bid

Section III: Certifications

Section IV: Additional Information

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

(c) In case the RFP specifies that files other than PDF are required in the bid, the Bidder must submit related files in attachment to the single epost Connect message above indicated. The maximum total size of the individual message is 1GB, including attachments.

(d) Format for Bid: Canada requests that bidders follow the format instructions described below in the preparation of their bid:

(i) use a numbering system that corresponds to the bid solicitation; and

(ii) include a title page at the front of each volume of the bid that includes the title, date, bid solicitation number, bidder's name and address and contact information of its representative.

3.2 Submission of Multiple Bids

(a) A Bidder, including related entities, will be permitted to submit only one bid in response to this bid solicitation. If a Bidder or any related entities participate in more than one bid (participating

means being part of the Bidder, not being a sub-contractor), Canada will provide those Bidders with 2 working days to identify the single bid to be considered by Canada. Failure to meet this deadline will result in all the affected bids being disqualified.

(b) For the purposes of this Article, regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law (whether that entity Is a natural person, corporation, partnership, etc), an entity will be considered to be "related" to a Bidder if:

(1) they are the same legal entity (i.e., the same natural person, corporation, partnership, limited liability partnership, etc.);

(2) they are "related persons" or "affiliated persons" according to the Canada Income Tax Act;

(3) the entities have now or in the two years before bid closing had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

(4) the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

(c) Individual members of a joint venture cannot participate in another bid, either by submitting a bid alone or by participating in another joint venture.

3.3 Joint Venture Experience

(a) Where the Bidder is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture.

Example: A bidder is a joint venture consisting of members L and O. A bid solicitation requires that the bidder demonstrate experience providing maintenance and help desk services for a period of 24 months to a customer with at least 10,000 users. As a joint venture (consisting of members L and O), the bidder has previously done the work. This bidder can use this experience to meet the requirement. If member L obtained this experience while in a joint venture with a third party N, however, that experience cannot be used because the third party N is not part of the joint venture that is bidding.

(b) A joint venture bidder may rely on the experience of one of its members to meet any given technical criterion of this bid solicitation.

Example: A bidder is a joint venture consisting of members X, Y and Z. If a solicitation requires: (a) that the bidder have 3 years of experience providing maintenance service, and (b) that the bidder have 2 years of experience integrating hardware with complex networks, then each of these two requirements can be met by a different member of the joint venture. However, for a single criterion, such as the requirement for 3 years of experience providing maintenance services, the bidder cannot indicate that each of members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-responsive.

(c) Joint venture members cannot pool their abilities with other joint venture members to satisfy a single technical criterion of this bid solicitation. However, a joint venture member can pool its individual experience with the experience of the joint venture itself. Wherever substantiation of a criterion is required, the Bidder is requested to indicate which joint venture member satisfies the requirement. If the Bidder has not identified which joint venture member satisfies the requirement, the Contracting Authority will provide an opportunity to the Bidder to submit

this information during the evaluation period. If the Bidder does not submitted this information within the period set by the Contracting Authority, its bid will be declared non-responsive.

Example: A bidder is a joint venture consisting of members A and B. If a bid solicitation requires that the bidder demonstrate experience providing resources for a minimum number of 100 billable days, the bidder may demonstrate that experience by submitting either:

- Contracts all signed by A;
- Contracts all signed by B; or
- Contracts all signed by A and B in joint venture, or
- Contracts signed by A and contracts signed by A and B in joint venture, or
- Contracts signed by B and contracts signed by A and B in joint venture.

That show in total 100 billable days.

(d) Any Bidder with questions regarding the way in which a joint venture bid will be evaluated should raise such questions through the Enquiries process as early as possible during the bid solicitation period.

3.4 Section I: Technical Bid

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

(i) 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 respond and address the requirements 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

(b) The technical bid consists of the following:

(i) **Bid Submission Form:** Bidders are requested to include the Bid Submission Form – Form 1 with their bids. It provides a common form in which Bidders can provide information required for evaluation and contract award, such as a contact name and the Bidder's Procurement Business Number, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Bid Submission Form is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so.

(ii) **Technical Documentation:** The Bidder is requested to provide technical documentation such as user manuals, screenshots, video demonstrations, design or system management documents (or other information sources) to support the Bidder's response to each requirement (a soft copy of the technical documents required to support the Technical Bid is acceptable). Links to websites are not acceptable and if provided to validate a mandatory requirement, it may render the bid response non-compliant. Any reference material listed by the Bidder to demonstrate compliance on a criteria is requested to be part of the bid (soft copy). If it is not included in the bid, it will not be taken into consideration by Canada. Where the reference is not located, Canada

may request that the Bidder direct Canada to the appropriate location in the bid documentation.

(iii) **Previous Similar Projects:** Where the bid is to include a description of previous similar projects: (i) a project must have been completed by the Bidder itself (and cannot include the experience of any proposed subcontractor or any affiliate of the Bidder); (ii) each project description should include, at minimum, the name and either the telephone number or e-mail address of a customer reference; and (iii) if more similar projects are provided than requested, Canada will decide in its discretion which projects will be evaluated. A project will be considered "similar" to the Work to be performed under any resulting contract if the project was for the performance of work that closely matches the descriptions identified in Annex A- Statement of Work. Work will be considered to "closely match" if the work in the provided project is described in at least 50% of the points of responsibility listed in the description of the given resource category.

(iv) **Customer Reference Contact Information:**

i. The Bidder should provide customer references. The customer reference is required to confirm, “if” requested by PSPC, the facts identified in the Bidder's bid.

The form of question to be used to request confirmation from customer references is as follows:

[Sample Question to Customer Reference: "Has [the Bidder] provided your organization with [describe the services and, if applicable, describe any required time frame within which those services must have been provided]?"

____ Yes, the Bidder has provided my organization with the services described above.

____ No, the Bidder has not provided my organization with the services described above.

____ I am unwilling or unable to provide any information about the services described above.]

For each customer reference, the Bidder should, at a minimum, provide the name and e-mail address for a customer contact person If only the telephone number is provided, it will be used to call to request the e-mail address and the reference check will be done by e-mail.

Bidders are also requested to include the title of the customer contact person. It is the sole responsibility of the Bidder to ensure that it provides a customer contact who is knowledgeable about the services the Bidder has provided to the customer and who is willing to act as a customer reference. Crown references will be accepted.

(v) **List of Proposed Software that will form part of the Solution**: The Bidder is requested to include a complete list identifying both the name and the version number of each component of the Software required for the proposed Solution. If the list of proposed Licensed Software is not included with the bid, it must be delivered to the Contracting Authority prior to Contract Award.

(vi) **Software Release Strategy:** The Bidder is requested to include a proposed Release Strategy, which should demonstrate that the Bidder's Release Strategy meets all the requirements for handling described in the Statement of Work.

(vii) **Solution System Architecture:** The Bidder is requested to include an overview of the proposed Software Solution's technical architecture. This is requested for information purposes only and will not be evaluated.

(viii) **Description of Evolution of Proposed Solution Components**: The Bidder is requested to describe when and how each of the components of the proposed **Solution** were conceived and how they have evolved, with the accomplishments of each release. This is requested for information purposes only and will not be evaluated.

(ix) **Sandbox Solution:** The Bidder should provide a sandbox Solution, as applicable, in accordance with Annex J – Technical Evaluation.

3.5 Section II: Financial Bid

(a) **Financial Bid:** Bidders must submit their financial bid in accordance with Basis of Payment in Annex B without any conditions, assumptions, or restrictions. Any financial bid that purports to restrict the way in which Canada acquires goods or services under the resulting contract, with the exception of those limitations that are expressly set out in this solicitation, may be considered non-responsive. The total amount of Applicable Taxes must be shown separately. Unless otherwise indicated, the Bidder is requested to include a firm all-inclusive price quoted in Canadian dollars in each cell requiring an entry in the pricing tables.

(b) **Exchange Rate Fluctuation:** The requirement does not offer exchange rate fluctuation risk mitigation. Requests for exchange rate fluctuation risk mitigation will not be considered.

(c) **Variation in Resource Rates by Time Period:** For any given resource category, where the financial tables provided by Canada allow different firm rates to be charged for a resource category during different time periods. The rate bid for the same resource category during any subsequent time period should not be lower than the rate bid for the time period that includes the first option year of the Contract.

(d) **Blank Prices:** Bidders are requested to insert "$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price blank, Canada will treat the price as "$0.00" for evaluation purposes and may request that the Bidder confirm that the price is, in fact, $0.00. No bidder will be permitted to add or change a price as part of this confirmation. Any bidder who does not confirm that the price for a blank item is $0.00 will be declared non-responsive.

(e) **Financial Submission:** The financial bid must include all costs for the requirement described in the bid solicitation for the entire Contract Period, including any option to extend the Contract Period. Bidders are required to submit prices, including prices associated with the necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation as per Annex B- Basis of Payment.

(f) **Electronic Payment of Invoices – Bid:** If you are willing to accept payment of invoices by Electronic Payment Instruments, complete Annex I – Bidders Forms, Form 8 – Electronic Payment Instruments, to identify which ones are accepted.

If Annex I – Bidders Forms, Form 8 – Electronic Payment Instruments is not completed, it will be considered as if Electronic Payment Instruments are not being accepted for payment of invoices. Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.

3.6 Section III: Certifications

It is a requirement that Bidders submit the certifications and additional information required under Part 5.

3.7 Section IV: Additional Information

3.7.1 Bidder's Proposed Sites or Premises Requiring Safeguarding Measures

As indicated in Part 1 under Security Requirements, the Bidder must provide the full addresses of the Bidder's and proposed individuals sites or premises for which safeguarding measures are required for Work Performance:

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

The Company Security Officer must ensure through the Contract Security Program that the Contractor and individuals hold a valid security clearance at the required level, as indicated in Part 1, clause 1.1, Security Requirements.

Bidders are requested to indicate this information on their Bid Submission Form.

3.7.2 Supply Chain Integrity (SCI) Requirements

Bidders must meet the SCI requirements described in Annex F - Supply Chain Integrity Process. The Supply Chain Security Information provided will be used by Canada to assess whether, in its opinion, a Bidder's proposed supply chain creates the possibility that the Bidder's proposed Solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information in accordance with Annex F- Supply Chain Integrity Process.

3.7.3 Consideration of Additional Software Use Terms included in Bid

1. Acceptance of all the terms and conditions contained in Part 7 - Resulting Contract Clauses (including those relating to software licensing and those incorporated by reference) is a mandatory requirement of this bid solicitation.

2. However, Bidders may, as part of their bid, submit additional software use terms. Whether or not those software use terms will be included in any resulting contract (as an Annex in accordance with the Article entitled "Priority of Documents" in the Resulting Contract Clauses) will be determined using the process described below. Whether or not any proposed additional software use terms are acceptable to Canada is a matter solely within the discretion of Canada. The process is as follows:
   (i) Bids may include additional software use terms that are proposed to supplement the terms of the Resulting Contract Clauses. Bidders should not submit a software publisher's full standard license terms (because full standard license terms generally contain provisions that deal with more than simply how the software can be used; for example, they frequently deal with issues such as limitation of liability or warranty, neither of which are software use terms);
   (ii) In cases where the Bidder has submitted a software publisher's full standard license terms, Canada will require that the Bidder remove these terms and

submit only the software use terms that the Bidder would like Canada to consider;

(iii) Canada will review any additional software use terms proposed by the top-3 ranked Bidders (identified after the financial evaluation) to determine if there are any provisions proposed by a Bidder(s) that are unacceptable to Canada;

(iv) If Canada determines that any proposed software use term by a Bidder is unacceptable to Canada, Canada will notify the Bidder, in writing, and will provide the Bidder with an opportunity to remove that provision from its bid or to propose alternate language for consideration by Canada. Canada may set a time limit for the Bidder to respond; if the Bidder submits alternate language, if Canada does not find the alternate language acceptable, Canada is not required to allow the Bidder to submit further alternate language;

(v) If the Bidder refuses to remove provisions unacceptable to Canada from its bid within the time limit set by Canada in its notice, the bid will be considered non-responsive and be disqualified; Canada may then proceed to the next-ranked bid; and

(vi) If the Bidder agrees to remove the provisions that are unacceptable to Canada and it is awarded any resulting contract, the proposed additional software use terms (as revised) will be incorporated as an annex to the contract, as set out in the Article entitled "Priority of Documents" in the Resulting Contract Clauses.

3. For greater certainty and to ensure that only additional software use terms that have been approved by both parties are incorporated into any resulting contract, unless the additional software use terms proposed by the Bidder are included as a separate annex to the Contract and initialed by both parties, they will not be considered part of any resulting contract (even if they are part of the bid that is incorporated by reference into the resulting contract). The fact that some additional terms and conditions or software use terms were included in the bid will not result in those terms applying to any resulting contract, regardless of whether or not Canada has objected to them under the procedures described above.

PART 4 – EVALUATION AND ASSESSMENT PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) The evaluation will be conducted in a structured, consistent, unbiased, fair and transparent manner. The objective of the evaluation is a well-supported determination of the Bid providing best value to Canada.

(b) Bids will be evaluated in accordance with the entire requirements of the bid solicitation including the Technical and Financial requirements. On completion of the bid evaluations, up to 3 top ranked responsive Bidders will be considered for the award of a Contract for Phase 1 work to develop a prototype Solution for a Capability and Usability Assessment (CUA).

(c) There will be several stages in the evaluation and selection process. Even though the evaluation, selection and assessment will be conducted in stages, the fact that Canada has proceeded to a later stage in its evaluations or assessments does not mean that Canada has conclusively determined that the Bidder or Contractor has successfully passed all the previous stages. Canada may conduct steps of the evaluation or assessment in parallel.

(d) The evaluation and teams will be composed of representatives of the Client and PSPC to evaluate and assess the bids and Prototypes on behalf of Canada. Canada may hire any independent consultant(s), or use any Government resources to evaluate any bid and assess any Prototypes. Not all members of either evaluation or assessment team will necessarily participate in all aspects of the respective stage evaluation or assessment.

(e) In addition to any other time periods established in the bid solicitation:

(1) **Requests for Clarifications:** If Canada seeks 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 Canada. Failure to meet this deadline will result in the bid being declared non-responsive.

(2) **Requests for Further Information:** If Canada requires additional information in order to do any of the following pursuant to the Section entitled "Conduct of Evaluation" in 2003, Standard Instructions - Goods or Services – Competitive Requirements:

I. verify any or all information provided by the Bidder in its bid; or
II. contact any or all references supplied by the Bidder (e.g., references named in the résumés of individual resources) to verify and validate any information submitted by the Bidder,

The Bidder must provide the information requested by Canada within 2 working days (or a longer period if specified in writing by the Contracting Authority). Failure to meet this deadline or provide further information as requested may result in the bid being declared non-responsive.

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

(f) Canada will use the Phased Bid Compliance Process described below.

4.1.1. Phased Bid Compliance Process (PBCP)

4.1.1.1 General

(a) Canada will conduct the PBCP described below for this requirement. Notwithstanding any review by Canada at Phase I or II of the PBCP, Bidders are and will remain solely responsible for the accuracy, consistency and completeness of their Bids and Canada does not undertake, by reason of this review, any obligations or responsibility for identifying any or all errors or omissions in Bids or in responses by a Bidder to any communication from Canada.

THE BIDDER ACKNOWLEDGES THAT THE REVIEWS IN PHASE I AND II OF THIS PBCP ARE PRELIMINARY AND DO NOT PRECLUDE A FINDING IN PHASE III THAT THE BID IS NON-RESPONSIVE, EVEN FOR MANDATORY REQUIREMENTS WHICH WERE SUBJECT TO REVIEW IN PHASE I OR II AND NOTWITHSTANDING THAT THE BID HAD BEEN FOUND RESPONSIVE IN SUCH EARLIER PHASE. CANADA MAY DEEM A BID TO BE NON-RESPONSIVE TO A MANDATORY REQUIREMENT AT ANY PHASE.

THE BIDDER ALSO ACKNOWLEDGES THAT ITS RESPONSE TO A NOTICE OR A COMPLIANCE ASSESSMENT REPORT (CAR) (EACH DEFINED BELOW) IN PHASE I OR II MAY NOT BE SUCCESSFUL IN RENDERING ITS BID RESPONSIVE TO THE MANDATORY REQUIREMENTS THAT ARE THE SUBJECT OF THE NOTICE OR CAR, AND MAY RENDER ITS BID NON-RESPONSIVE TO OTHER MANDATORY REQUIREMENTS.

(b) Canada may, in its discretion, request and accept at any time from a Bidder and consider as part of the Bid, any information to correct errors or deficiencies in the Bid that are clerical or administrative, such as, without limitation, failure to sign the Bid or any part or to checkmark a box in a form, or other failure of format or form or failure to acknowledge; failure to provide a procurement business number or contact information such as names, addresses and telephone numbers; inadvertent errors in numbers or calculations that do not change the amount the Bidder has specified as the price or of any component thereof that is subject to evaluation. This shall not limit Canada's right to request or accept any information after the bid solicitation closing in circumstances where the bid solicitation expressly provides for this right. The Bidder will have the time period specified in writing by Canada to provide the necessary documentation. Failure to meet this deadline will result in the Bid being declared non-responsive.

(c) The PBCP does not limit Canada's rights under Standard Acquisition Clauses and Conditions (SACC) 2003 (2020-05-28) Standard Instructions – Goods or Services – Competitive Requirements nor Canada's right to request or accept any information during the solicitation period or after bid solicitation closing in circumstances where the bid solicitation expressly provides for this right, or in the circumstances described in subsection (b).

(d) Canada will send any Notice or CAR by any method Canada chooses, in its absolute discretion. The Bidder must submit its response by the method stipulated in the Notice or CAR. Responses are deemed to be received by Canada at the date and time they are delivered to Canada by the method and at the address specified in the Notice or CAR. An email response permitted by the Notice or CAR is deemed received by Canada on the date and time it is received in Canada's email inbox at Canada's email address specified in the Notice or CAR. A Notice or CAR sent by Canada to the Bidder at any address provided by the Bidder in or pursuant to the Bid is deemed received by the Bidder on the date it is sent by Canada. Canada is not responsible for late receipt by Canada of a

response, however caused.

4.1.1.2 Phase I of the PBCP: Financial Bid

(a) After the closing date and time of this bid solicitation, Canada will examine the Bid to determine whether it includes a Financial Bid and whether any Financial Bid includes all information required by the solicitation. Canada's review in Phase I will be limited to identifying whether any information that is required under the bid solicitation to be included in the Financial Bid is missing from the Financial Bid. This review will not assess whether the Financial Bid meets any standard or is responsive to all solicitation requirements.

(b) Canada's review in Phase I will be performed by the Contracting Authority.

(c) If Canada determines, in its absolute discretion that there is no Financial Bid or that the Financial Bid is missing all of the information required by the bid solicitation to be included in the Financial Bid, then the Bid will be considered non-responsive and will be given no further consideration.

(d) For Bids other than those described in c), Canada will send a written notice to the Bidder ("Notice") identifying where the Financial Bid is missing information. A Bidder, whose Financial Bid has been found responsive to the requirements that are reviewed at Phase I, will not receive a Notice. Such Bidders shall not be entitled to submit any additional information in respect of their Financial Bid.

(e) The Bidders who have been sent a Notice shall have the time period specified in the Notice (the "Remedy Period") to remedy the matters identified in the Notice by providing to Canada, in writing, additional information or clarification in response to the Notice. Responses received after the end of the Remedy Period will not be considered by Canada, except in circumstances and on terms expressly provided for in the Notice.

(f) In its response to the Notice, the Bidder will be entitled to remedy only that part of its Financial Bid which is identified in the Notice. For instance, where the Notice states that a required line item has been left blank, only the missing information may be added to the Financial Bid, except that, in those instances where the addition of such information will necessarily result in a change to other calculations previously submitted in its Financial Bid, (for example, the calculation to determine a total price), such necessary adjustments shall be identified by the Bidder and only these adjustments shall be made. All submitted information must comply with the requirements of this solicitation.

(g) Any other changes to the Financial Bid submitted by the Bidder will be considered to be new information and will be disregarded. There will be no change permitted to any other Section of the Bidder's Bid. Information submitted in accordance with the requirements of this solicitation in response to the Notice will replace, in full, **only** that part of the original Financial Bid as is permitted above, and will be used for the remainder of the bid evaluation process.

(h) Canada will determine whether the Financial Bid is responsive to the requirements reviewed at Phase I, considering such additional information or clarification as may have been provided by the Bidder in accordance with this Section. If the Financial Bid is not found responsive for the requirements reviewed at Phase I to the satisfaction of Canada, then the Bid shall be considered non-responsive and will receive no further consideration.

(i) Only Bids found responsive to the requirements reviewed in Phase I to the satisfaction of Canada, will receive a Phase II review.

4.1.1.3 Phase II of the PBCP: Technical Bid

(a) Canada's review in Phase II of the PBCP will be limited to a review of the Technical Bid to identify any instances where the Bidder has failed to meet any Eligible Mandatory Criterion. This review will not assess whether the Technical Bid meets any standard or is responsive to all solicitation requirements. Eligible Mandatory Criteria are all mandatory technical criteria that are identified in this solicitation as being subject to the PBCP. Mandatory technical criteria that are not identified in the solicitation as being subject to the PBCP, will not be evaluated until Phase III of the PBCP.

(b) Canada will send a written notice to the Bidder (Compliance Assessment Report or "CAR") identifying any Eligible Mandatory Criteria that the Bid has failed to meet. A Bidder whose Bid has been found responsive to the requirements that are reviewed at Phase II will receive a CAR that states that its Bid has been found responsive to the requirements reviewed at Phase II. Such Bidder shall not be entitled to submit any response to the CAR.

(c) A Bidder shall have the period specified in the CAR (the "Remedy Period") to remedy the failure to meet any Eligible Mandatory Criterion identified in the CAR by providing to Canada in writing additional or different information or clarification in response to the CAR. Responses received after the end of the Remedy Period will not be considered by Canada, except in circumstances and on terms expressly provided for in the CAR.

(d) The Bidder's response must address only the Eligible Mandatory Criteria listed in the CAR as not having been achieved, and must include only such information as is necessary to achieve such compliance. Any additional information provided by the Bidder which is not necessary to achieve such compliance will not be considered by Canada, except that, in those instances where such a response to the Eligible Mandatory Criteria specified in the CAR will necessarily result in a consequential change to other parts of the Bid, the Bidder shall identify such additional changes, provided that its response must not include any change to the Financial Bid.

(e) The Bidder's response to the CAR should identify in each case the Eligible Mandatory Criterion in the CAR to which it is responding, including identifying in the corresponding section of the original Bid, the wording of the proposed change to that section, and the wording and location in the Bid of any other consequential changes that necessarily result from such change. In respect of any such consequential change, the Bidder must include a rationale explaining why such consequential change is a necessary result of the change proposed to meet the Eligible Mandatory Criterion. It is not up to Canada to revise the Bidder's Bid, and failure of the Bidder to do so in accordance with this subparagraph is at the Bidder's own risk. All submitted information must comply with the requirements of this solicitation.

(f) Any changes to the Bid submitted by the Bidder other than as permitted in this solicitation, will be considered to be new information and will be disregarded. Information submitted in accordance with the requirements of this solicitation in response to the CAR will replace, in full, **only** that part of the original Bid as is permitted in this Section.

(g) Additional or different information submitted during Phase II permitted by this section will be considered as included in the Bid, but will be considered by Canada in the evaluation of the Bid at Phase II only for the purpose of determining whether the Bid meets the Eligible Mandatory Criteria. It will not be used at any Phase of the evaluation to increase or decrease any score that the original Bid would achieve without the benefit of such additional or different information. For instance, an Eligible Mandatory Criterion that requires a mandatory minimum number of points to achieve compliance will be assessed at Phase II to determine whether such mandatory minimum score would be achieved with such additional or different information submitted by the Bidder in response to the CAR. If so, the Bid will be considered responsive in respect of such Eligible Mandatory Criterion, and the additional or different information submitted by the Bidder shall bind the Bidder as part of its Bid, but the Bidder's original score, which was less than the mandatory minimum for such Eligible Mandatory Criterion, will not change, and it will be that original score that is used to calculate any score for the Bid.

(h) Canada will determine whether the Bid is responsive for the requirements reviewed at Phase II, considering such additional or different information or clarification as may have been provided by the Bidder in accordance with this Section. If the Bid is not found responsive for the requirements reviewed at Phase II to the satisfaction of Canada, then the Bid shall be considered non-responsive and will receive no further consideration.

(i) Only Bids found responsive to the requirements reviewed in Phase II to the satisfaction of Canada, will receive a Phase III evaluation.

4.1.1.4 (2018-03-13) Phase III of the PBCP: Final Evaluation of the Bid

(a) In Phase III of the PBCP, Canada will complete the evaluation of all Bids found responsive to the requirements reviewed at Phase II. Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria.

(b) A Bid is non-responsive and will receive no further consideration if it does not meet all mandatory evaluation criteria of the solicitation.

4.1.2 Evaluation

4.1.2.1 Mandatory Technical Criteria:

(a) The Phased Bid Compliance Process (PBCP) will apply to all mandatory technical criteria listed in Annex J, Technical Evaluation.

(b) The mandatory criteria that will be evaluated as part of the bid evaluation are listed in Annex J- Technical Evaluation. Bidders are required to address clearly and in sufficient details all mandatory evaluation criteria against which their Bids will be evaluated. Simply repeating the statement contained in the Mandatory criteria is not sufficient.

(c) Each bid will be reviewed to determine whether it meets the mandatory requirements of the bid solicitation. Any element of the bid solicitation identified with the words "must" or "mandatory" is a mandatory requirement. Subject to the PBCP, Bids that do not comply with each mandatory requirement will be declared non-responsive and be disqualified.

(d) Claims in a bid that a future upgrade or release of any of software included in the bid will meet the mandatory requirements of the bid solicitation, where the upgrade or release is not available at bid closing, will not be considered.

4.1.2.2 Point-rated Technical Criteria:

(a) The point-rated criteria that will be evaluated as part of the bid evaluation are listed in Annex J- Technical Evaluation. Subject to the Phased Bid Compliance Process (PBCP), a bidder must obtain a minimum of 70% of the total score for the technical evaluation criteria stipulated in Annex J, Technical Evaluation which are subject to point rating.

(b) Each bid will be rated by assigning a score to the rated requirements, which are identified in the bid solicitation by the word "rated" or by reference to a score. Bidders who fail to submit complete bids with all the information requested by this bid solicitation will be rated accordingly. The point-rated technical criteria are described in Annex J- Technical Evaluation.

4.1.2.3 Reference Checks:

(a) For reference checks, Canada will conduct the reference check in writing by e-mail. Canada will send all e-mail reference check requests to contacts supplied by all the Bidders on the same day using the e-mail address provided in the bid. Canada will not award any points and/or a bidder will not meet the mandatory experience requirement (as applicable) unless the response is received within 5 working days of the date that Canada's e-mail was sent.

(b) On the third working day after sending out the reference check request, if Canada has not received a response, Canada will notify the Bidder by e-mail, to allow the Bidder to contact its reference directly to ensure that it responds to Canada within 5 working days. If the individual named by a Bidder is unavailable when required during the evaluation period, the Bidder may provide the name and e-mail address of an alternate contact person from the same customer. Bidders will only be provided with this opportunity once for each customer, and only if the originally named individual is unavailable to respond (i.e., the Bidder will not be provided with an opportunity to submit the name of an alternate contact person if the original contact person indicates that he or she is unwilling or unable to respond). The Bidder will have 24 hours to submit the name of a new contact. That contact will again be given 5 working days to respond once Canada sends its reference check request.

(c) Wherever information provided by a reference differs from the information supplied by the Bidder, the information supplied by the reference will be the information evaluated.

(d) Points will not be allocated and/or a bidder will not meet the mandatory experience requirement (as applicable) if (1) the reference customer states he or she is unable or unwilling to provide the information requested, or (2) the customer reference is not a customer of the Bidder itself (for example, the customer cannot be the customer of an affiliate of the Bidder instead of being a customer of the Bidder itself). Nor will points be allocated or a mandatory met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Bidder.

(e) Whether or not to conduct reference checks is discretionary. However, if PSPC chooses to conduct reference checks for any given rated or mandatory requirement, it will check the references for that requirement for all Bidders who have not, at that point, been found non-responsive.

4.1.2.4 Financial Evaluation:

(a) Bidders must submit their financial bid in accordance with the Basis of Payment in Annex B and it is provided for bid evaluation price determination only. The estimates used to calculate the Total Bid Price in Annex B are estimates only and are not to be considered as a commitment from Canada.

(b) **Formulae in Pricing Tables.** If the pricing tables provided to Bidders in Annex B include any formulae, Canada may re-input the prices provided by Bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a Bidder.

(c) **Substantiation of Professional Services Rates**. In Canada's experience, Bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates bid for professional services, Canada may, but will have no obligation to, require price support in accordance with this Article. If Canada requests price support, it will be requested from all otherwise responsive Bidders who have proposed a rate that is at least 20% lower than the median rate bid by all responsive Bidders for the relevant resource category or categories. If Canada requests price support, the Bidder must provide the following information:

(i) an invoice (referencing a contract serial number or other unique contract identifier) that shows that the Bidder has provided and invoiced a customer (with whom the Bidder deals at arm's length) for services performed for that customer similar to the services that would be provided in the relevant resource category, where those services were provided for at least three months within the twelve months before the bid solicitation closing date, and the fees charged were equal to or less than the rate offered to Canada;

(ii) in relation to the invoice in (i), evidence from the Bidder's customer that the services identified in the invoice include at least 50% of the tasks listed in the Statement of Work for the category of resource being assessed for an unreasonably low rate. This evidence must consist of either a copy of the contract (which must describe the services to be provided and demonstrate that at least 50% of the tasks to be performed are the same as those to be performed under the Statement of Work in this bid solicitation) or the customer's signed certification that the services subject to the charges in the invoice included at least 50% of the same tasks to be performed under the Statement of Work in this bid solicitation;

(iii) in respect of each contract for which an invoice is submitted as substantiation, a résumé for the resource that provided the services under that contract that demonstrates that, in relation to the resource category for which the rates are being substantiated, the resource would meet the mandatory requirements and achieve any required pass mark for any rated criteria; and

(iv) the name, telephone number and, if available, e-mail address of a contact person at the customer who received each invoice submitted under (i), so that Canada may verify any information provided by the Bidder.

Once Canada requests substantiation of the rates bid for any resource category, it is the sole responsibility of the Bidder to submit information (as described above and as otherwise may be requested by Canada, including information that would allow Canada to verify information with the resource proposed) that will allow Canada to determine whether it can rely, with

confidence, on the Bidder's ability to provide the required services at the rates bid. If Canada determines that the information provided by the Bidder does not adequately substantiate the unreasonably low rates, the bid will be declared non-responsive.

1. Number of Resource Categories Evaluated: All resource categories proposed will be evaluated as part of this bid solicitation. Additional resources will only be assessed after Contract award once specific tasks are requested of the Contractor. After Contract award, the Task Authorization process will be in accordance with Part 7 - Resulting Contract Clauses, the Article titled "Task Authorization". When a Task Authorization Form (TA Form) is issued, the Contractor will be requested to propose a resource to satisfy the specific requirement based on the TA Form's Statement of Work.

2. Corrections: Canada may, at its discretion, request and accept at any time from a Bidder and consider as part of the Bid, any information to correct errors or deficiencies in the Bid that are clerical or administrative such as, without limitation, failure to sign the Bid or any part or to checkmark a box in a form, or other failure of format or form or failure to acknowledge; failure to provide a procurement business number or contact information such as names, addresses and telephone numbers; inadvertent errors in numbers or calculations that do not change the amount the Bidder has specified as the price or of any component thereof that is subject to evaluation. This shall not limit Canada's right to request or accept any information after the Bid required submission date in circumstances where the RFP expressly provides for this right. The Bidder will have the time period specified in writing by Canada to provide the necessary documentation. Failure to meet this deadline will result in the Bid being declared non-compliant.

4.1.2.5 Ranking Bids:

(a) Highest Combined Rating of Technical merit (70%) and Price (30%) – Evaluation Stage

Following Canada's evaluation of the technical and financial bids, the top 3 ranked bids will be determined based on the highest responsive combined rating of technical merit and price. 70% weightage will be given to the technical bid and 30% weightage will be given to the financial bid as per the following formula:

$$\frac{\text{Total points received by bidder for rated requirements}}{\text{Maximum technical rated score possible}} \times 70\% = \text{Total 1}$$

$$\frac{\text{Lowest Total Bid Price}}{\text{Total Bid Price of the bid being ranked}} \times 30\% = \text{Total 2}$$

Sum of (Total 1) and (Total 2) = Combined Rating of Technical Merit and Price.

Evaluation Stage Components	Overall Weighting
Technical bid Score	70%
Financial bid Score	30%

Top-ranked responsive bids will be determined based on the proposal, which has met all mandatory requirements and offers the Highest Responsive Combined Rating of Technical Merit and Price as calculated above.

4.1.2.6 Basis of Selection:

(a) To be declared responsive, a bid must:

(i) comply with all the requirements of the bid solicitation;
(ii) meet all mandatory technical requirements stipulated in Annex J- Technical Evaluation; and,
(iii) obtain the required minimum of 70% score for the technical evaluation criteria stipulated in Annex J, Technical Evaluation which are subject to point rating.

Subject to the Phased Bid Compliance Process, Bids not meeting i), ii) or iii) will be declared non-responsive.

(b) Bids will be ranked by score from highest to lowest and up to the 3 top ranked responsive bids will be recommended for award of a Contract. For each of the top 3 ranked compliant bidders, Canada will award up to 3 Contracts valued at $200,000 CAD each, applicable taxes extra. The Contractors will be required to perform the Work defined in Phase 1 of Annex A Statement of Work.

(c) In the event that a Bidder withdraws their bid, or a bid is set aside, Canada may offer the next highest ranked responsive Bidder a Contract.

(d) In the event of a tie score(s) that impacts the ranking, the responsive Bidder with the highest Technical Score will be recommended for award of a Contract.

(e) Bidders should note that all contract awards are subject to Canada's internal approval process, which includes a requirement to approve funding in the amount of any proposed contract. Despite the fact that the Bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.

4.2 Rights of Canada

Canada reserves the right to:

(a) reject any or all bids received in response to the bid solicitation;

(b) enter into negotiations with Bidders on any or all aspects of their bids;

(c) accept any bid in whole or in part without negotiations;

(d) cancel the bid solicitation at any time;

(e) cancel and reissue the bid solicitation at any time;

(f) if no responsive bids are received and the requirement is not substantially modified, reissue the bid solicitation by inviting only the Bidders who bid to resubmit bids within a period designated by Canada; and,

(g) negotiate with the sole responsive Bidder to ensure the best value to Canada.

4.3 Rejection of Bids

(a) Grounds for Rejection. Canada may reject a bid where the Bidder is bankrupt or where its activities are rendered inoperable for an extended period, or where the Bidder or an employee or subcontractor included as part of the bid:

(i) is subject to a Vendor Performance Corrective Measure, under the Vendor Performance Corrective Measure Policy, which renders the Bidder, employee or subcontractor ineligible to bid on the requirement;

(ii) has committed fraud, bribery, fraudulent misrepresentation or failed to comply with laws protecting individuals against any manner of discrimination;

(iii) has conducted himself/herself improperly; with respect to current or prior transactions with the Government of Canada;

(iv) has been suspended or terminated by Canada for default with respect to a contract;

(v) has performed other contracts in a sufficiently poor manner so as to jeopardize the successful completion of the requirement being bid on.

(b) Notification of Rejection for Suspension or Termination. Where Canada intends to reject a bid due to suspension, termination or sufficiently poor performance of another contract, the Contracting Authority will so inform the Bidder and provide the Bidder 10 days within which to make representations, before making a final decision on the bid rejection.

(c) Multiple Bids from Single Bidder or Joint Venture. Canada reserves the right to apply additional scrutiny, in particular, when multiple bids are received in response to a bid solicitation from a single bidder or a joint venture. Canada reserves the right to reject any or all of the bids submitted by a single bidder or joint venture if their inclusion:

(i) in the evaluation has the effect of prejudicing the integrity and fairness of the process, or

(ii) in the procurement process would distort the solicitation evaluation or would not provide good value to Canada.

4.4 Capability and Usability Assessment Procedures

(a) **Prototype Development Engagement Sessions:** Following the bid evaluations and award of up to 3 Contracts for Work to develop a prototype Solution in accordance with Phase 1- Prototype Solution of Annex A-Statement of Work and the CUA criteria described in Appendix A to Annex A–Statement of Work, Canada will engage Contractors in the development of their Prototype solutions by conducting Contractor engagement sessions in accordance with procedures described in Appendix A to Annex A-Statement of Work.

(b) Canada will in the contractor engagement sessions provide feedback on the prototypes as these are being developed by the Contractors. The engagements are expected to provide Contractors a thorough understanding of Canada's requirements for an innovative Solution with feedback from users at the forefront. The sessions would be conducted in the same manner for each Contractor to allow each Contractor the same opportunity to demonstrate and seek feedback or input to their prototype work. It is a requirement of this agile approach that each Contractor participate in the engagement sessions throughout the prototype development process.

(c) During the Prototype development phase, all Contractor enquiries all Contractor enquiries must be submitted in writing to the Contracting Authority for redress by Canada. 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 Contractor do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered with copies to all Contractors. Enquiries not submitted in a form that can be distributed to all Contractors may not be answered by Canada.

(d) Capability and Usability Assessment (CUA): A CUA assessment will be conducted following the Contractors submission of a prototype solution in accordance with Phase 1- Prototype Solution of Annex A-Statement of Work and the CUA criteria described in Appendix A to Annex A – Statement of Work.

(e) Contractors will be required to submit all contract deliverables for Phase 1 Work including a CUA Prototype Solution in the format and by the date specified in the contract for Canada's assessment against the CUA criteria described in Appendix A to Annex A – Statement of Work.

(f) The Contractor's CUA Prototype Solution will be assessed against point rated CUA criteria. The point rated CUA criteria will be scored and the sum of the scores for each individual category will be calculated in accordance with the assessment criteria and maximum points listed in each category of Appendix A to Annex A – Statement of Work.

(g) The overall assessment score for the CUA will be calculated based on the highest responsive combined rating of technical merit, price and CUA.

(h) Requests for Clarifications or Further information: If Canada seeks clarification or requires additional information from the Contractor in order to verify any or all information provided by the Contractor or to complete Canada's assessment of the Contractor's proposed solution, the Contractor must provide the necessary information requested by Canada within 24 hours (or a longer period if specified in writing by the Contracting Authority). Failure to respond by the specified deadline may result in the Contractor's solution not being given further consideration by Canada. If additional time is required by the Contractor, the Contracting Authority may grant an extension in his or her sole discretion.

(i) Basis of Canada's Decision to Exercise the Phase 2 Full Solution Option

The top ranked responsive CUA Prototype Solution will be determined based on the Contractor having satisfied all the requirements under Phase 1-Prototype Solution of the Contract, including submitting all required deliverables and obtaining the highest responsive combined rating of technical merit, price and CUA. 10% weighting will be given to the Technical Evaluation Score. 30% weighting will be given to the Financial Evaluation Score. 60% weighting will be given to the CUA Score, as per the following table:

Assessment Components	Overall Weighting
Technical Evaluation Score*	10%
Financial Evaluation Score*	30%
Capability and Usability Assessment Score	60%

**NOTE: The Technical and Financial evaluation scores referenced in the above table are the scores obtained from the bid evaluation stage on which basis the contract(s) to develop the Prototype solution is awarded.*

(i) In the event of a tie, the CUA Score will be used to rank the Contractors from highest to lowest score. If there are further ties, the lowest Financial Score will be used to rank the Contractor.

(ii) Prototype on Platform (PoP) Test for Top-Ranked CUA Contractor:

a. Through the Prototype on Platform (PoP) test, Canada may, at its discretion, test the solution proposed by the top-ranked Contractor (identified after the CUA assessment) to confirm both that it will function and integrate as described within the RCMP's environment and that it meets the technical functionality requirements described in Appendix A – Capability and Usability Assessment (CUA) to the Statement of Work - Annex A of the contract. If requested by Canada, the PoP test will take place at a site in the National Capital Region provided by Canada that recreates the technical environment described in Section 4.6 - RCMP Cloud Deployment to Annex A - Statement of Work. The contractor is required to have a team of support personal at location to assist the RCMP with the installation and integration.

b. After being notified by the Contracting Authority for a PoP test, the Contractor will be given a maximum of 10 working days to start the preparation to move the prototype to the RCMP's designated environment. During this preparation time:

i. The contractor must provide all documentation and instructions for the installation and integration of the prototype into RCMP's Protected B Cloud Tenant.
ii. The contractor must identify all required tools that will be part of the installation and integration.
iii. The contractor must identify the representative(s) of the support team that will assist RCMP with the installation and integration in RCMP's location.
iv. The Contractor must package and deliver the prototype in a way that enables RCMP to begin the installation on the date specified.

c. Canada will document the results of the PoP Test. If Canada determines that the proposed solution does not meet any mandatory requirement of the PoP Test, the Contractor will be considered to have failed the PoP Test and given no further consideration. With the top-ranked Contractor having failed the PoP Test, Canada may, at its discretion, consider the second-ranked Contractor (identified after the CUA assessment) to conduct a PoP Test of their proposed solution.

d. In connection with the PoP testing, the Contractor grants to Canada a limited license to use the Contractor's proposed software solution for testing and assessment purposes.

e. If, during the initial installation of the software for the PoP test, the Contractor discovers that there are missing and/or corrupt files for software components identified in the technical bid, the Contractor must cease the installation process and inform the Contracting Authority. If the Contracting Authority determines

that the missing and/or corrupt files are for components identified in the technical bid, the Contractor may be permitted to submit to the Contracting Authority the missing files and/or replacements for the corrupt files on electronic media or by referring to a web site where the files can be downloaded. These files must have been commercially released to the public 10 calendar days before the date of the scheduled PoP test. Upon receiving the files on electronic media or downloading them from a corporate web site, the Contracting Authority will verify that (i) the files were commercially released to the public 10 calendar days before the date of the scheduled PoP test; (ii) the files do not include new releases or versions of the software; (iii) the files belong to software components identified in the technical bid; and (iv) the software will not need to be recompiled to make use of the files. The Contracting Authority will have the sole discretion to decide if the additional files may be installed for the PoP test. Under no circumstances will files required to correct flaws in the software programming or code be permitted. This process can be used only a single time, and only during the initial installation of the software for the PoP test.

(iii) Having completed all the assessments, Canada will, at its sole discretion, exercise its irrevocable option to select a Contractor to perform all or a portion of the Work under article 3. Phase 2 - Solution of Annex A – Statement of Work. Canada may also, at its discretion, exercise its irrevocable option with other Contractors who participated in the CUA for all or a portion of the Work if it is determined that this would best meet the needs of Canada.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

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

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

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

5.1 Certifications Required with Bid

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

(a) **Integrity Provisions – Declaration of Convicted Offences**

In accordance with the Integrity Provisions of the Standard Instructions, all Bidders must provide with their bid, **if applicable**, the Integrity declaration form available on the Forms (Form 5) for the Integrity Regime website (http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html) to be given further consideration in the procurement process.

(b) **Professional Services Resources**

(i) By submitting a bid, the Bidder certifies that, if it is awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives.

(ii) By submitting a bid, the Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

(iii) By submitting a bid, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

(c) **Software Publisher Certification, Software Publisher Authorization and Software Contributor Certification**

(i) If the Bidder is the Software Publisher for any of the proprietary software products it bids, Canada requires that the Bidder confirm in writing that it is the Software Publisher. Bidders are requested to use the Software Publisher Certification Form included with the bid solicitation. Although all the contents of the Software Publisher Certification Form are required, using the form itself to provide this information is not mandatory. For

Bidders who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided. Alterations to the statements in the form may result in the bid being declared non-responsive.

(ii) Any Bidder that is not the Software Publisher of all the proprietary software products proposed in its bid is required to submit proof of the Software Publisher's authorization, which must be signed by the Software Publisher (not the Bidder). No Contract will be awarded to a Bidder who is not the Software Publisher of all of the proprietary software it proposes to supply to Canada, unless proof of this authorization has been provided to Canada. If the proprietary software proposed by the Bidder originates with multiple Software Publishers, authorization is required from each Software Publisher. Bidders are requested to use the Software Publisher Authorization Form included with the bid solicitation. Although all the contents of the Software Publisher Authorization Form are required, using the form itself to provide this information is not mandatory. For Bidders/Software Publishers who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided. Alterations to the statements in the form may result in the bid being declared non-responsive.

(iii) In this bid solicitation, "Software Publisher" means the owner of the copyright in any software products proposed in the bid, who has the right to license (and authorize others to license/sub-license) its software products.

(iv) The following certification documents are required as part of the Submission:

Form 2 Software as a Service Publisher Certification Form
Form 3 Software as a Service Publisher Authorization Form
Form 4 Cloud Service Provider (“CSP”) Letter of Attestation

5.2 Certifications Precedent to Contract Award and Additional Information

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

5.2.1 Supply Chain Integrity Process

(1) During the RFP process, the Contract period and any resulting Option periods, the Supply Chain Security Authority identified by Canada, may assess the Bidder’s Supply Chain Security Information (SCSI) based on its National Security mandate to protect Canada’s IT infrastructure as well as to assess threats, risks and vulnerabilities.

(2) Canada will assess whether, in its opinion, the Bidder’s supply chain creates the possibility that the Bidder’s supply chain or proposed solution could compromise or be used to compromise the security integrity of Canada’s equipment, firmware, software, systems or information, or represents a threat to Canada’s National Security, in accordance with Annex F- Supply Chain Integrity Process.

(3) It is a condition precedent to any contract award that a Bidder successfully satisfy the Security Authority’s Supply Chain Integrity assessment.

5.2.2 IT Assessment

It is a condition precedent to any contract award that a Bidder complete the Canadian Center for Cyber Security (CCCS) IT Assessment program.

5.3 Integrity Provisions – Required Documentation

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

5.4 Federal Contractors Program for Employment Equity – Bid Certification

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

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 (Form 7) titled Federal Contractors Program for Employment Equity – Certification, before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity – Certification, for each member of the Joint Venture.

5.5 Sole Bid – Price Support

In the event that your bid is the sole bid received, Government Contract Regulations require price support be submitted in conjunction with the offer. Acceptable price support is one or more of the following:

(a) a current published price list indicating the percentage discount available to Canada; or

(b) copies of paid invoices for the like quality and quantity of the goods, services or both sold to other customers; or

(c) a price breakdown showing the cost of direct labour, direct materials, purchased items, engineering and plant overheads, general and administrative overhead, transportation, etc., and profit; or

(d) price or rate certifications; or

(e) any other supporting documentation as requested by Canada.

PART 6 – SECURITY AND FINANCIAL REQUIREMENT

Prior to award of contract, the following conditions must be met:

6.1 Canadian Suppliers:

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

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

(c) The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED B, including an IT Link at the level of PROTECTED B.

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

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

(i) Security Requirements Check List and security guide (if applicable), attached at Annex C;
(ii) Industrial Security Manual (Latest Edition)

6.2 Foreign Supplier

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the

Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PSPC. The Canadian DSA is the authority confirming Bidder compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient Bidder incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing the Solution, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified below in Protection and Security of Data Stored in Databases.

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

(b) The foreign recipient Bidder must provide proof that they are incorporated or authorized to do business in their jurisdiction as indicated in Part 7 – Resulting Contract Clauses.

(c) The foreign recipient Bidder must be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or operating and authorized to do business, as indicated in Part 7 – Resulting Contract Clauses, 7.5(b) Security Requirement for Foreign Suppliers.

(d) The foreign recipient Bidders must provide assurance that it can receive and store CANADA PROTECTED B/Personal information/assets on its site or premises as indicated in Part 7 – Resulting Contract Clauses and the listed IT Security Requirements.

(e) The foreign recipient Bidder's proposed location of work performance must meet the security requirement as indicated in Part 7 and as listed in the IT Security Requirements.

(f) The foreign recipient Bidder must provide the address(es) of proposed location(s) of work performance and document safeguarding.

(g) The successful foreign recipient Bidder's proposed individuals requiring access to CANADA PROTECTED/Personal information/assets or restricted work sites must EACH hold a valid Criminal Record Check, with favorable results, from a recognized governmental agency or private sector organization in their country, as well as a Background Verification, validated by the Canadian DSA.

(h) The successful foreign recipient Bidder's proposed individuals must not begin the Work until all requisite security requirements have been met.

(i) In the case of a joint venture Bidder, each member of the joint venture must meet the security and privacy requirements.

(j) The foreign recipient Bidders must provide proof that all the databases including the backup database used by organizations to provide the services described in the SOW containing any CANADA PROTECTED/Personal Information, related to the Work, are located in Canada.

(k) The successful foreign recipient Bidder MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system any CANADA PROTECTED B/Personal information/assets until authorization to do so has been confirmed by the Canadian DSA.

(l) The Bid must clearly indicate the Work which the foreign recipient Bidder plans to subcontract. All subcontracting arrangements which provide the subcontractor with access to any CANADA PROTECTED/Personal Information are subject to approval by Canada. The description of subcontracting arrangements should demonstrate how the foreign recipient Bidder will ensure that all requirements, terms, conditions, and clauses of the subcontract are met.

(m) In the event that a foreign recipient Bidder is chosen as a Contractor for this contract, subsequent country-specific foreign security requirement clauses must be generated and promulgated by the Canadian DSA, and provided to the Government of Canada Contracting Authority, to ensure compliance with the security provisions.

6.3 Financial Capability

SACC Manual clause A9033T (2012-07-16) Financial Capability applies, except that subsection 3 is deleted and replaced with the following: "If the Bidder is a subsidiary of another company, then any financial information required by the Contracting Authority in 1(a) to (f) must also be provided by each level of parent company, up to and including the ultimate parent company. The financial information of a parent company does not satisfy the requirement for the provision of the financial information of the Bidder; however, if the Bidder is a subsidiary of a company and, in the normal course of business, the required financial information is not generated separately for the subsidiary, the financial information of the parent company must be provided. If Canada determines that the Bidder is not financially capable but the parent company is, or if Canada is unable to perform a separate assessment of the Bidder's financial capability because its financial information has been combined

with its parent's, Canada may, in its sole discretion, award the contract to the Bidder on the condition that one or more parent companies grant a performance guarantee to Canada."

PART 7 – RESULTING CONTRACT CLAUSES

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

This Contract is made on [CONTRACT DATE] between [CONTRACTOR NAME] (the "Contractor") and [GOVERNMENT OF CANADA ENTITY] ("Canada").

7.1 Requirement

(a) The Contractor agrees to provide to the Client the work, goods and services described in the Contract (including the Annex A - Statement of Work -SOW-) in accordance with and at the prices set out in the Contract. This includes at a minimum:

SOW Phase 1: All work and deliverables associated with Phase 1- Prototype Solution, including the Contractors participation in the contractor engagement sessions, and Prototype on Platform (PoP) Test process if applicable, and;

SOW Phase 2 (if applicable): As and when duly authorized, all work and deliverables associated with Phase 2 Full Solution,

Which all includes, but not limited to:

i. granting user access or user license or both , as applicable, to use the Solution for 100 users during SOW Phase 1 Prototype Solution, and up to 2000 users (including 500 concurrently), for Phase 2 Final Solution if applicable;

ii. performing any Work required to design or develop features or functionality, and develop and implement any commercially available or custom software components for the Prototype Solution, and the Full Solution, if applicable;

iii. providing any Solution-related software applications and components required for accessing and using the Prototype Solution, and the Full Solution if applicable, on-line and within the Client's environment, if applicable, in accordance with the Contractor's Solution delivery model;

iv. setting-up and adjusting, as applicable, the Prototype Solution, and the Full Solution if applicable, in the Cloud and within Client's environment in accordance with the Contractor's Solution delivery model;

v. maintaining and updating the Full Solution if applicable, of all Solution computational resource service(s) and component(s) under Contractor's responsibility in accordance with the Contractor's Solution delivery model;

vi. managing incidents and defects, of the Full Solution if applicable, occurring to any Solution computational resource component(s) under Contractor's responsibility in accordance with the Contractor's Solution delivery model, in order to ensure the Solution operate optimally at the applicable service levels;

vii. providing the Prototype Solution, and Full Solution if applicable, operating documentation, training and maintenance documentation in accordance with the Contractor's Solution delivery model;

viii. providing a 12-month warranty for any Solution-related software component(s) operating within Client's environment, if applicable, in accordance with the Contractor's Solution delivery model;

ix. providing plans, reports, meetings, design, modeling, management, training, assessments, technical expertise, documentation and support services linked to development, implementation, deployment and transition of a licensed Solution; and

x. providing professional services and additional training services, as and when requested by Canada, in accordance with the Task authorization (TA) process described herein.

(b) **Optional Goods and Services**

The Contractor grants to Canada the right to exercise the following irrevocable options to acquire goods and services. Options are detailed the Annex A – Statement of work and prices are set out under Annex B – Basis of Payment. All options will be exercised by the Contracting Authority and, will be evidenced, through a contract amendment. The Contracting Authority may exercise any option at any time before the expiry of the Contract by sending a written notice to the Contractor. This includes at a minimum:

i. Option to implement and deliver the full Solution in accordance with Phase 2 work described in Annex A- Statement of Work, including providing plans, reports, meetings, design, modeling, testing, assessments, technical expertise, documentation and support services linked to the development, implementation, deployment and transition of the Full Solution in accordance with the Contractor's Solution delivery model. The Contractor agrees that it will be paid in accordance with the applicable provisions set out in Annex B – Basis of Payment;
ii. Option to acquire, at Canada's sole discretion, additional user licenses or additional user accesses or both, as applicable, in accordance with Annex A – Statement of Work and at the price set out under Annex B- Basis of Payment;
iii. Option to acquire via Task Authorization on an as and when requested basis Professional Services and Training in accordance with Annex A Statement of Work and at the prices set out under Annex B – Basis of Payment; and
iv. Option to acquire via Task Authorization on an as and when requested basis Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both (if applicable), in accordance with Annex A - Statement of Work and at the prices set out under Annex B - Basis of Payment.

The option(s) will be exercised, under the same terms and conditions and at the prices and rates stated in Annex B – Basis of Payment, by the Contracting Authority and will be evidenced, through a contract amendment.

The Contracting Authority may exercise any option at any time before the expiry of the Contract by sending a written notice to the Contractor.

(c) **Client**: Under the Contract, the "Client" is the RCMP. However, the Contracting Authority can add additional Clients from time to time, which may include any department or Crown corporation as described in the Financial Administration Act (as amended from time to time), and any other party for which Public Services and Procurement Canada may be authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act.

(d) **Reorganization:** The Contractor's obligation to provide the Services and perform the Work will not be affected by (and no additional fees will be payable as a result of) any form of

reorganization or restructuring of any Client. Canada may designate replacement Contracting Authority or Technical Authority.

(e) **Evolution and Use of Solution:** While the Contract(s) is of a specific duration, Canada reserves the right to continue to Contract for and leverage this Solution for as long as it makes business sense for Canada to do so. Canada also expects that the Solution will evolve with time and technologies, including incorporation of functionalities or technologies that isn't currently part of the requirement. Canada reserves the right to consider these evolutionary functionalities or technologies to be part of the ongoing scope of the work being done under the Contract, subject to Canada's internal approval processes. Canada reserves the right to, at a subsequent date and at its sole discretion, identify the solution either as a multi-departmental solution, or designate the solution as a Government of Canada Enterprise-wide standard if and when determined by the GC-Enterprise Architecture Review Board (GCEARB).

(f) **Definitions and Interpretations:** The definitions and interpretations are included in the Annex D – Definitions and Interpretations.

(g) **License to Material Subject to Copyright**: In this section, "Material" means anything that is created or developed by the Contractor as part of the Work under the Contract, and in which copyright subsists.

i. The Contractor grants to Canada a non-exclusive, perpetual, irrevocable, world-wide, fully-paid and royalty-free license to exercise all rights comprised in the copyright in the Material, for any government purposes. Canada may use independent contractors in the exercise of Canada's license pursuant to this clause.

ii. Copyright in any translation of the Material made by or for Canada belongs to Canada. Canada agrees to reproduce the Contractor's copyright notice, if any, on all copies of the Material, and to acknowledge the Contractor's title to the copyright in the original Work on all copies of translations of the Material effected by or for Canada.

iii. No restrictions other than those set out in this section must apply to Canada's use of copies of the Material or of translated versions of the Material.

iv. At the request of Canada, the Contractor must provide to Canada, at the completion of the Work or at such other time as Canada may require, a written permanent waiver of moral rights, in a form acceptable to Canada, from every author that contributed to the Material. If the Contractor is an author of the Material, the Contractor permanently waives its moral rights in respect of the Material.

(h) **General Conditions and Supplemental General Conditions**

(i) General Conditions

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

ii. 2030 (2020-05-28), General Conditions - Higher Complexity - Goods, apply to and form part of the Contract.

iii. 2035 (2020-05-28), General Conditions - Higher Complexity – Services, apply to and form part of the Contract.

(ii) Supplemental General Conditions

The following Supplemental General Conditions below are incorporated in the resulting Contract:

i. 4003 (2010-08-16), Supplemental General Conditions - Licensed Software;

ii. 4004 (2013-04-25), Supplemental General Conditions - Maintenance and Support Services for Licensed Software;

iii. 4006 (2010-08-16) Contractor to Own Intellectual Property Rights in Foreground Information; and

iv. 4008 (2008-12-12) Personal Information.

7.2 Contract Term

(a) **Contract Period.** The Contract Period includes the entire period of time during which the Contractor is obliged to provide the goods and services and to perform the Work.

(b) **Initial Term:** This Contract begins on the date the Contract is awarded for a period of 3 years from contract award date. The Contractor must immediately commence Work on Phase 1 of Annex A-Statement of Work following the award of the contract by the Contracting Authority.

(c) **Option to extend Contract Period:** The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 8 additional one-year periods under the same terms and conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in Annex B – Basis of Payment. Canada may exercise the option(s) at any time before the expiry of the Contract by sending a written notice to the Contractor. The option may be exercised only by the Contracting Authority, and will be evidenced, for administrative purposes only, through an amendment to the Contract.

(d) **Delivery Dates:** The Contractor must provide all deliverables in accordance with the associated delivery dates as detailed under Phase 1 of Annex A – Statement of Work. If Canada exercised its irrevocable option for the Contractor to implement and deliver the Full Solution, the Contractor must provide all deliverables in accordance with the associated delivery dates as detailed under Phase 2 of Annex A – Statement of Work.

(e) **Additional Options:**

(i) **Option to Exercise Phase 2:** The Contractor grants to Canada the irrevocable option to authorize the Contractor to perform the Work detailed under article 3. “Phase 2 – Full Solution” of Annex A – Statement of Work. The Contractor agrees that it will be paid in accordance with the applicable provisions set out in Annex B – Basis of Payment;

(ii) **Option to purchase Additional User Licenses or Additional User Access or both, as applicable:** The Contractor grants to Canada the irrevocable option to acquire Additional User Licenses or User Accesses or both, as applicable, under the same terms and conditions. The Contractor agrees that it will be paid in accordance with the applicable provisions set out in Annex B – Basis of Payment;

(iii) **Option to acquire Professional Services** on an as-and-when-requested basis as detailed in Annex A Statement of Work and at the prices set out under Annex B – Basis of Payment;

(iv) **Option to acquire Training Services** on an as-and-when-requested basis as detailed in Annex A Statement of Work and at the prices set out under Annex B – Basis of Payment; and

(v) **Option to acquire, Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both (if applicable)** on an as-and-when-requested basis in accordance with Annex A - Statement of Work and at the prices set out under Annex B - Basis of Payment.

7.3 Solution

(a) **Solution Software.** The Contractor must deliver the Solution as indicated in subsection 7.1.

(b) **Software Application Evolution; Features or Functionalities.** Canada acknowledges that the Solution, underlying software application or associated infrastructure may evolve during the course of the Contract Period. The Contractor agrees to continue to provide the Services as the commercially available Solution, with functionality or features and on with terms that are no less favourable than as at the time of Contract award.

(c) **Improvements to and Evolution of the Solution.** The parties acknowledge that technology and business models evolve quickly and that any Solution provided at the beginning of the Contract Period inevitably will be different from the Solution provided at the end of the Contract Period and the method(s) by which the Solution and any potential peripherals are delivered to Canada are likely to change or evolve and that, at the time of entering into this Contract, the parties cannot possibly contemplate all the goods or services that may be delivered under this Contract, other than they will be connected to delivering to Users. With that in mind, the parties agree that:

i. The Contractor must maintain and continuously improve the Solution and infrastructure throughout the Contract Period on a commercially reasonable basis, and must provide those improvements and enhancements to Canada as part of Canada's subscription and license whenever applicable, with no price adjustment if those improvements and enhancements are also offered to other customers at no additional cost.

ii. If the Contractor removes any functions from the commercial offering to the Solution and offers those functions in any new or other services or products, the Contractor must continue to provide those functions to Canada as part of Canada's subscription and license, whenever applicable, to the Services, under the existing terms and conditions of the Contract regardless of whether those other services or products also contain new or additional functions. Contractor has no obligation to comply with this paragraph if the Solution acquired by Canada is still offered by Contractor in parallel with the new services offered to other customers.

(d) **Downgrade.** If the Contractor is unable to provide the Services with no less favourable features and functionality, the Contractor will provide written Notice to Canada identifying the circumstance, and alternative options, specifically including a reduction in pricing. If no proposed alternative option is acceptable to Canada, the Contractor agrees to consent to a termination of the Contract, and pay all identifiable direct costs incurred by Canada to migrate and store Client's Data, and to procure equivalent replacement services.

(e) **Maintenance Releases.** During the Software Support Period, the Contractor must provide to Canada all Maintenance Releases, in object-code form, at no additional cost. All Maintenance Releases will become part of the Solution and will be subject to the conditions of Canada's license with respect to the Solution. Unless provided otherwise in the Contract, Canada will receive at least one Maintenance Release during any twelve (12) month maintenance period.

7.4 Solution Operational Changes

(a) The Government of Canada is seeking an innovative **Solution** that can adapt and evolve with technological advances throughout the duration of the Contract. The Contractor-delivered **Solution** must be extensible and adaptable to harness future technology innovations that the Contractor may use to upgrade their Licensed Software. The Contractor will be required to provide to the Government of Canada all technological upgrades to the **Solution** free of charge where:

(i) The upgrade has been made to their Licensed Software; and
(ii) The upgrade has been given free of charge to the Contractor's other client(s).

(b) The Government of Canada also requires the Contractor to ensure that the **Solution** remains compatible with all future versions of iOS, Android and the following Web browsers:

- Internet Explorer
- Google Chrome
- Firefox
- Safari

(c) The Government of Canada requires that the Solution remains compliant with the WET and WCAG, as defined in the Statement of Work, throughout the duration of the Contract.

(d) **On-going Maintenance of Software Code**: The Contractor must continue to maintain the **Solution** (i.e., the version or "build" originally accepted and licensed under the Contract). For clarity, the Contractor or the software publisher must be continuing to develop new code in respect of the components of the **Solution** to maintain its functionality, enhance it, and deal with Software Errors for at least 1 year from the date the **Solution** is accepted in accordance with the Acceptance Criteria of Annex A – Statement of Work. After that time, if the Contractor or the software publisher decides to discontinue or no longer maintain the then-current version or "build" of any component of the **Solution** and, instead, decides to provide upgrades to any Licensed Software component as part of the Software Support, the Contractor must provide written notice to Canada at least 12 months in advance of the discontinuation.

7.5 Solution Maintenance and Support

(a) The Contractor must continuously maintain and support the Solution.

(b) **Solution Support.** The Solution Support includes the following Technical Hotline Support and Web Support services:

i. **Technical Hotline Support:** the Contractor must provide the Technical Hotline Support through the Contractor's toll-free hotline at (INSERT AT CONTRACT AWARD), in English and French, from 8:00 A.M. to 5:00 P.M. Eastern Time, Monday to Friday (excluding statutory holidays observed by the federal government in the province from which the call is made). The Contractor must answer or return all calls (with a live service agent) within

60 minutes of the initial time of the Client or User's initial call. The Contractor's personnel must be qualified and able to respond to the Client's and any Client User's questions and, to the extent possible, be able to resolve user problems over the telephone and provide advice regarding configuration problems relating to the Licensed Software.

ii. **Web Support:** The Contractor must provide Canada with technical web support services through a website that must include, as a minimum, frequently asked questions and on-line software diagnostic routines, support tools, and services. The Contractor's website must provide support in English. The Contractor's website must be available to Canada's users 24 hours a day, 365 days a year, and must be available 99% of the time. The Contractor's website address is (INSERT AT CONTRACT AWARD).

(c) **Software Error Correction Services**

i. Canada may report to the Contractor any failure of the Licensed Programs to operate in accordance with the Software Documentation or, if applicable, the Specifications during the Software Support Period. Canada may report failures either in writing or by telephone or other remote communication. Upon receipt of a report of a failure from Canada, unless provided otherwise in the Contract, the Contractor must use all reasonable efforts to provide Canada within the time frames established in subsections ii and iii, with a correction of the Software Error which caused the failure. Any such software correction must cause the Solution to meet the Software Documentation or, if applicable, the Specifications during the Software Support Period. The Contractor must use all reasonable efforts to provide permanent corrections for all Software Errors and the Contractor warrants that the Solution will meet the functional and performance criteria set out in the Specifications. All Software Error corrections will become part of the Solution and will be subject to the conditions of Canada's license with respect to the Solution.

ii. Unless provided otherwise in the Contract, the Contractor must respond to a report of a Software Error in accordance with the severity of the Software Error, as detailed in subsection iii. The severity will be reasonably determined by Canada, and communicated to the Contractor, based on the following definitions:

"Severity 1":

indicates total inability to use a Licensed Program, resulting in a critical impact on user objectives;

"Severity 2":

indicates ability to use a Licensed Program but user operation is severely restricted;

"Severity 3":

indicates ability to use a Licensed Program with limited functions which are not critical to overall user operations;

"Severity 4":

indicates that the problem has been by-passed or temporarily corrected and is not affecting user operations.

iii. Unless provided otherwise in the Contract, the Contractor must use reasonable efforts to correct Software Errors as follows:

"Severity 1":

within twenty-four (24) hours of notification by Canada;"

Severity 2":

within seventy-two (72) hours of notification by Canada;

"Severity 3":

within fourteen (14) days of notification by Canada;

"Severity 4":

within ninety (90) days of notification by Canada.

iv. If Canada reports a Software Error to the Contractor, Canada must give the Contractor reasonable access to the computer system on which the Licensed Program resides, and must provide such information as the Contractor may reasonably request, including sample output and other diagnostic information, in order to permit the Contractor to expeditiously correct the Software Error.

7.6 Contractor Use of Canada's Data

(a) The Contractor is provided access to use, for the term of the Contract, to Canada's Data for the sole and exclusive purpose of providing the **Solution** to Users, including a license to collect, process, store, generate, and display Canada Data only to the extent necessary in the providing of the Services.

(b) The Contractor must:

(i) keep and maintain Canada's Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Agreement and applicable law to avoid unauthorized access, use, disclosure, or loss;

(ii) use and disclose Canada's Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with the Contract and applicable law; and,

(iii) not use, sell, rent, transfer, distribute, or otherwise disclose or make available Canada's Data for the Contractor's own purposes or for the benefit of anyone other than Canada without Canada's prior written consent.

(iv) provide Canada full access to all Solution Data

The Contractor, its subcontractors, and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

If requested by the Technical Authority, the Contractor must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The Contractor must not begin using a form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.

At the time it requests Personal Information from any individual, if the Contractor doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the Contractor must ask the Technical Authority for instructions.

7.7 Services

Solution Services

(i) The Contractor will provide all Services required for Canada to access and use the Solution as specified in Annex A – Statement of Work.

(ii) **Authority.** The Contractor represents and warrants that it owns or has obtained and will maintain throughout the Contract Period, all necessary authority specifically including intellectual property rights required to provide the Services in accordance with the terms of this Contract.

(iii) **Indemnification.** The Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any intellectual property infringement claim by a third party based on Canada's use of the Solution.

(iv) **Accessibility:** The Contractor must ensure that the Solution does not interfere with accessibility standards compliance, as specified in the Standard on Web Accessibility: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601#

(v) **Included.** The Contractor represents and warrants that the Services include:

i. hosting and maintenance of the Solution, when applicable,

ii. provision of all incidental and additional required information technology infrastructure services, in compliance with all required security standards,

iii. the technical infrastructure that complies with all required security standards, allowing Canada to use the Solution to process any of Client's Data in compliance with its expressed security standards, and unfettered access and use by the Client, regardless of the amount of data created, processed or stored by the Solution,

all of which is included in the price.

(vi) **Restricted Usage Rights.** Canada acknowledges that in providing the Services, the Contractor is not delivering ownership rights to any software product, component of the Solution or infrastructure used by the Contractor to provide the Services, except as expressly provided in a Task Authorization. Canada will not knowingly:

i. distribute, license, loan, or sell the Solution;

ii. impair or circumvent the Solution's security mechanisms; or

iii. remove, alter, or obscure any copyright, trademark, or other proprietary rights notice on or in the Solution.

(vii) **Applicable Terms and Conditions**. The Contractor has advised and Canada acknowledges that the Contractor may unilaterally modify the terms under which it provides its commercial offering of the Solution, without notice to its customers, including Canada. The Contactor represents and warrants that any such modification will not result in less favorable terms, specifically including price, service levels and remedies, regardless of any notification to the contrary.

(viii) **Additional Terms and Conditions.** The parties agree that any terms and conditions, including any "click-through" or "pop-up" notices, that apply to the Contractor's commercial offering of the Solution, including third party tools or incidental infrastructure, will not apply to Canada's use of the Solution if those terms conflict with

the express terms of this Contract. The terms and conditions of third party tools not specified the Contract are not subject to this section.

7.8 Documentation

(a) **Solution Documentation.** The Contractor must provide or deliver access to the commercially available Solution Documentation to Canada upon Contract Award. The Contractor must update Solution Documentation on a commercially reasonable basis.

(b) **Other Documentation**. The Contractor must provide or deliver access to any documentation required in performance of the Work.

(c) **Translation Rights**. The Contractor agrees that Canada may translate any written deliverable, including the Solution Documentation or Training Materials into English or French. The Contractor acknowledges that Canada owns any translation and is under no obligation to provide it to the Contractor. Canada will include any copyright and/or proprietary right notice that was part of the original document in any translation. The Contractor will not be responsible for technical errors that arise as a result of any translation made by Canada.

(d) **Moral Rights.** At the request of Canada, the Contractor may provide a written permanent waiver of moral rights, in a form acceptable to Canada, from every author that contributed to the written deliverable. If the Contractor is unable or unwilling to obtain the requested waivers, the Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any moral rights infringement claim by a third party based on Canada's translation of written documentation.

(e) **Defective Documentation**. If at any time during the Contract Period, Canada advises the Contractor a defect or non-conformance in any part of the documentation delivered with the Work, the Contractor will correct the defect or non-conformance must as soon as possible and at its own expense. Canada may provide the Contractor with information about defects or non-conformance in other documentation, including the Solution Documentation, for information purposes only.

7.9 Optional Professional Services, Training Services, Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both (if applicable).

(a) **Professional Services.** The Contractor must perform and deliver such Professional Services (the "Work") to Canada on an as-and-when requested basis as detailed in a Task Authorization.

(b) **Training Services.** The Contractor must perform and deliver such Training Services (the "Work") to Canada on an as-and-when requested basis as detailed in a Task Authorization.

(c) **Optional Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both (if applicable).** The Contractor must perform and deliver such support services (the "Work") to Canada on an as-and-when requested basis as detailed in a Task Authorization.

(d) **Conduct of the Work; Warranty.** The Contractor represents and warrants that (a) it is competent to perform the Work, (b) it has everything necessary to perform the Work, including the resources, facilities, labour, technology, equipment, and materials; and (c) it has the

necessary qualifications, including knowledge, skill, know-how and experience, to effectively perform the Work.

(e) **Time is of the Essence.** It is essential that the Work be delivered within or at the time stated in a Task Authorization.

(f) **Authorized Personnel.** All the Work must be performed solely by Contractor's authorized personnel.

(g) **Key Personnel.** If specific individuals are identified in the Contract to perform the Work, the Contractor must provide the services of those individuals. If the Contractor is unable to provide the services of any specific individual identified in the Contract, it must provide a replacement with equivalent qualifications and experience and provide written notice to Canada giving (i) the reason for the replacement, (ii) the name and qualifications of the replacement individual, and (iii) proof that the proposed replacement has the required security clearance from Canada.

(h) **Request to Replace Key Personnel.** The Contracting Authority may order that a replacement stop performing the Work. In such a case, the Contractor must immediately comply with the order and secure a further replacement in accordance with terms of replacement of key personnel. The fact that the Contracting Authority does not order that a replacement stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.

(i) **Migration.** The Contractor acknowledges that the nature of the Services provided under the Contract, Canada may require continuity. Prior to the transition to the new contractor or to Canada, the Contactor must provide all operational, technical, design and configuration information and documentation for all Services required to complete the transition, provided that it is not Contractor confidential information. The Contractor represents and warrants that it will not directly or indirectly interfere with or impede Canada's access to or transfer of Client's Data.

(j) **Migration and Transition Services.** The Contractor agrees that, in the period leading up to the end of the Contract Period, if Migration or Transition Services are requested by Canada, it will diligently assist Canada in the transition from the Contract to a new contract with another supplier and or migrate Client's Data to a new supplier environment, that there will be no charge for the services below other than those charges set out in the Basis of Payment.

7.10 Remedies

(a) **Work.** If at any time during the Contract Period the Work fails to meet its warranty obligations, the Contractor must as soon as possible correct at its own expense any errors or defects and make any necessary changes to the Work.

(b) **Documentation.** If at any time during the Contract Period, Canada discovers a defect or non-conformance in any part of the documentation delivered with the Work, the Contractor must as soon as possible correct at its own expense the defect or non-conformance.

(c) **Canada's Right to Remedy**. If the Contractor fails to fulfill any obligation described herein within a reasonable time of receiving a notice, Canada will have the right to remedy or to have remedied the defective or non-conforming Work at the Contractor's expense. If Canada does

not wish to correct or replace the defective or non-conforming Work, an equitable reduction will be made in the Contract Price.

7.11 Subcontracts

(a) **Conditions to Subcontracting.** The Contractor may subcontract the performance of the Work, provided (a) the Contractor obtains the Contracting Authority's prior written consent, (b) the subcontractor is bound by the terms of this Contract, and (c) the Contractor remains liable to Canada for all the Work performed by the subcontractor.

(b) **Exceptions to Subcontracting Consent.** The Contractor is not required to obtain consent for subcontracts specifically authorized in the Contract. The Contractor may also without the consent of the Contracting Authority: (i) purchase "off-the-shelf" items and any standard articles and materials that are ordinarily produced by manufacturers in the normal course of business (ii) subcontract any incidental services that would ordinarily be subcontracted in performing the Work; and (iii) permit its subcontractors at any tier to make purchases or subcontract as permitted in paragraphs (i) and (ii).

7.12 Excusable Delay

(a) No Liability. The Contractor will not be liable for performance delays nor for non-performance due to causes beyond its reasonable control that could not reasonably have been foreseen or prevented by means reasonably available to the Contractor, provided the Contractor advises the Contracting Authority of the occurrence of the delay or of the likelihood of the delay as soon as the Contractor becomes aware of it (referred to as an "Excusable Delay").

(b) Notice. The Contractor must also advise the Contracting Authority, within 15 business days, of all the circumstances relating to the delay and provide to the Contracting Authority for approval a clear work around plan explaining in detail the steps that the Contractor proposes to take in order to minimize the impact of the event causing the delay.

(c) Delivery and Due Dates: Any delivery date or other date that is directly affected by an Excusable Delay will be postponed for a reasonable time that will not exceed the duration of the Excusable Delay.

(d) Canada not responsible for Costs: Unless Canada has caused the delay by failing to meet an obligation under the Contract, Canada will not be responsible for any costs incurred by the Contractor or any of its subcontractors or agents as a result of an Excusable Delay.

7.13 Right to Terminate.

(a) If such an event prevents performance under the Contract for more than 30 calendar days, then the Contracting Authority may elect to terminate the TA, or part or all of this Contract on a "no fault" basis, meaning neither party will be liable to the other in connection with the Excusable Delay or resulting termination, and Canada will only be responsible for paying for those services received up to the effective date of the termination.

7.14 Inspection and Acceptance of the Work

(a) Inspection by Canada: All the Work is subject to inspection and acceptance by Canada. Canada's inspection and acceptance of the Work does not relieve the Contractor of its

responsibility for defects or other failures to meet the requirements of the Contract. Canada will have the right to reject any work that is not in accordance with the requirements of the Contract and the Contractor is required to correct or replace it at its own expense.

(b) Acceptance Procedures: Unless provided otherwise in the Contract, the acceptance procedures are as follows:

a. when the Work is complete, the Contractor must notify the Technical Authority in writing, with a copy to the Contracting Authority, by referring to this provision of the Contract and requesting acceptance of the Work;

b. Canada will have 30 days from receipt of the notice to perform its inspection (the "Acceptance Period").

(c) Deficiencies and Resubmission of Deliverable: If Canada provides notice of a deficiency during the Acceptance Period, the Contractor must address the deficiency as soon as possible and notify Canada in writing once the Work is complete, at which time Canada will be entitled to re-inspect the Work before acceptance and the Acceptance Period will begin again. If Canada determines that a deliverable is incomplete or deficient, Canada is not required to identify all missing items or all deficiencies before rejecting the deliverable.

(d) Access to Locations: The Contractor must provide representatives of Canada access to all locations where any part of the Work is being performed, other than multi-tenant data centres, at any time during working hours. Representatives of Canada may make examinations and such tests of the Work as they may think fit. The Contractor must provide all assistance and facilities, test pieces, samples and documentation that the representatives of Canada may reasonably require for the carrying out of the inspection. The Contractor must forward such test pieces and samples to such person or location as Canada specifies.

(e) Contractor Inspection for Quality: The Contractor must inspect and approve any part of the Work before submitting it for acceptance or delivering it to Canada. All deliverables submitted by the Contractor must be of a professional quality, free of typographical and other errors, and consistent with the highest industry standards.

(f) Inspection Records: The Contractor must keep accurate and complete inspection records that must be made available to Canada on request. Representatives of Canada may make copies and take extracts of the records during the performance of the Contract and for up to three years after the end of the Contract.

(g) Informal Feedback: Upon request by the Contractor, Canada may provide informal feedback prior to any deliverable being formally submitted for acceptance. However, this must not be used as a form of quality control for the Contractor's Work. Canada is not obliged to provide informal feedback.

7.15 Kick-Off Meeting

(a) The Contractor must schedule a kick off meeting with the presence of the Client and PSPC Contracting Authority to discuss the overall requirement, the approach and methodology, contract, projects establishment, timeframe management and to clarify any issues. The

meeting must occur prior starting any work and at a mutually agreed location or by teleconference. The Chairperson of the meeting shall be the Contracting Authority.

(b) The Contractor must prepare and distribute the agenda of the meeting and submit it within a reasonable delay to the Contracting Authority for approval, prior to distribution to all Authorities.

(c) The Contractor must provide the agenda and a presentation, if applicable, within 2 business days prior to the start date of the meeting.

(d) The Contractor must prepare and provide minutes of the meeting within 2 business days to the Contracting Authority for approval, prior to distribution to all Authorities.

7.16 Progress Review Meeting

(a) The Contracting Authority and the Contractor may, at any time, convene a meeting to discuss and review the progress of the Work against this Contract. Any such meeting must occur following notice to the other Party and must normally be held by teleconference. The Chairperson of the meeting shall be the Contracting Authority or the Party requesting the meeting;

(b) The Contractor must prepare the agenda of the meeting and distribute it to all Authorities;

(c) The Contractor must prepare the agenda of the meeting and submit it within a reasonable delay to the Contracting Authority for approval, prior to distributing them to all Authorities;

(d) The Contractor will have to provide the completed presentation and items' agenda five (5) business days prior to the start date of the meeting;

(e) The Contractor must prepare minutes of meeting and submit them within 15 working days to the Contracting Authority for approval, prior to distributing them to all Authorities.

7.17 Task Authorization

(a) The Contractor's provision of professional services, training services, Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both (if applicable) performed under this Contract will be on an "as and when requested basis" using a Task Authorization.

(b) **Form and Content of TA.** A TA will contain (a) Contract and TA number, (b) the details of the required goods and services, activities and resources, (c) a description of the deliverables, (d) a schedule indicating completion dates for the major activities or submission dates for the deliverables, (e) security requirements, and (f) costs. A TA will follow the format detailed in Annex F – Task Authorization Forms.

(c) **Contractor's Response to TA.** The Contractor must provide to Canada, within the period specified in the TA, the proposed total price for performing the task and a breakdown of that cost, established in accordance with the fees. The Contractor will not be paid for preparing or providing its response or for providing other information required to prepare and validly issue the TA.

(d) **TA Limit and Authorities for Validly Issuing TA.** A validly issued TA must be signed by the appropriate Canadian Authority as set forth in this Contract. Any work performed by the Contractor without receiving a validly issued TA is done at the Contractor's own risk.

(e) **Periodic Usage Reports.** The Contractor must compile and maintain records on its provision of services to the federal government under the valid TA as issued under this Contract.

(f) **Consolidation of TA for Administrative Purposes.** This Contract may be amended from time to time to reflect all validly issued TA to date, to document the Work performed under those TA for administrative purposes.

7.18 Security Requirement

Canada reserve the right to update the security requirement.

(a) **Canadian Supplier**

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

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

(iii) The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED B, including an IT Link at the level of PROTECTED B.

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

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

i. Security Requirements Check List and security guide (if applicable), attached at Annex C;

ii. Industrial Security Manual (Latest Edition)

(b) **Foreign Supplier**

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

(i) The foreign recipient **Contractor / Subcontractor** must be from a Country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the

countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

(ii) The Foreign recipient **Contractor / Subcontractor** must at all times during the performance of the **contract/subcontract** be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or operating and authorized to do business. The Foreign recipient **Contractor / Subcontractor** must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and the Canadian DSA, and identify the relevant national Privacy Authority. For European **Contractors / Subcontractors**, this will be the national Data Protection Authority (DPA).

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

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

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

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

iv. The foreign recipient **Contractor / Subcontractor** must not grant access to **CANADA PROTECTED B/Personal** information/assets, except to its personnel subject to the following conditions:

1) Personnel have a need-to-know for the performance of the **contract/subcontract**;

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

3) The foreign recipient **Contractor / Subcontractor** must ensure that personnel provide consent to share results of the Criminal Record and Background Checks with the Canadian DSA and other Canadian Government Officials, if requested; and

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

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

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

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

(v) Until the Foreign recipient **Contractor / Subcontractor** has provided the Canadian DSA with the required written personnel security screening assurances, the Foreign recipient **Contractor / Subcontractor** personnel **MUST NOT HAVE ACCESS** to **CANADA PROTECTED A or B** information/assets, and **MUST NOT ENTER** "Government of Canada" or "Contractor" sites where such information/assets are kept, without an escort. An escort is defined as "a Government of Canada" or "Contractor" employee who holds the appropriate Personnel Security Clearance at the required level.

(vi) The foreign recipient **Contractor / Subcontractor** must, at all times during the performance of the **contract/subcontract** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED B**. All **CANADA PROTECTED/Personal** information, furnished to the foreign recipient **Contractor / Subcontractor** or produced by the foreign recipient **Contractor / Subcontractor**, must also be safeguarded as follows:

(vii) The foreign recipient **Contractor / Subcontractor** acknowledges and agrees that its obligations to safeguard, manage, and protect all Personal Information under the **contract / subcontract** are in addition to any obligations it has under national privacy legislation of the country(ies) in which it is incorporated or operates.

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

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

(x) The foreign recipient **Contractor / Subcontractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA**

PROTECTED/Personal information/ assets pursuant to this **contract** has been compromised.

(xi) The foreign recipient **Contractor / Subcontractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED/Personal** information/ assets accessed by the foreign recipient **Contractor / Subcontractor**, pursuant to this **contract**, have been lost or disclosed to unauthorized persons.

(xii) The foreign recipient **Contractor / Subcontractor** must not disclose **CANADA PROTECTED/Personal** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent must be sought through the Canadian DSA.

(xiii) The foreign recipient **Contractor / Subcontractor** must provide the **CANADA PROTECTED/Personal** information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.

(xiv) Upon completion of the Work, the foreign recipient **Contractor / Subcontractor** must return to the Government of Canada, all **CANADA PROTECTED/Personal** information/assets furnished or produced pursuant to this **contract/subcontract**, including all **CANADA PROTECTED** information/ assets released to and/or produced by its subcontractors.

(xv) The foreign recipient **Contractor / Subcontractor** requiring access to **CANADA PROTECTED/Personal** information/assets or Canadian restricted sites, under this contract, must submit a Request for Site Access to the Departmental Security Officer of the Royal Canadian Mounted Police**.**

(xvi) The foreign recipient **Contractor / Subcontractor** MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA PROTECTED B/Personal** information/assets until authorization to do so has been confirmed by the Canadian DSA.

(xvii) The foreign recipient **Contractor / Subcontractor** must ensure that the appropriate security clauses, as determined by the Canadian DSA, are inserted in all subcontracts that involve access to CANADA PROTECTED/Personal information provided to or generated under this **contract/ subcontract** and must ensure that the conditions placed on a subcontractor are no less favorable to Canada than the conditions set out in these security requirements.

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

(xix) Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.

(xx) The foreign recipient **Contractor / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex C.

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

(c) **Protection and Security of Data Stored in Databases**

(i) The foreign recipient **Contractor / Subcontractor** must ensure that all the databases used by organizations to provide the services described in the proposed Solution containing any **CANADA PROTECTED/Personal** information, related to the Work, are located in Canada.

(ii) The foreign recipient **Contractor / Subcontractor** must control access to all databases on which any data relating to the **contract / subcontract** is stored so that only individuals with the appropriate security screening are able to access the database, either by using a password or other form of access control (such as biometric controls).

(iii) The foreign recipient **Contractor / Subcontractor** must ensure that all databases on which any data relating to the **contract / subcontract** is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases.

(iv) The foreign recipient **Contractor / Subcontractor** must ensure that all data relating to the **contract/ subcontract** is processed only in Canada or in another country approved by the Contracting Authority under subsection (b) (i).

(v) The foreign recipient **Contractor / Subcontractor** must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented in writing to an alternate route. The Contracting Authority will only consider requests to route domestic traffic through another country that meets the requirements of subsection (b) (i).

(vi) Despite any section of the General Conditions relating to subcontracting, the foreign recipient **Contractor / Subcontractor** must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the contract unless the Contracting Authority (in collaboration with the Canadian DSA) first consents in writing.

(d) **Personal Information**

(i) **Interpretation**

i. In the **contract / subcontract**, unless the context otherwise requires,

"General Conditions" means the general conditions that form part of the **contract / subcontract**;

"Personal Information" means information about an individual, including the types of information specifically described in the *Privacy Act*, R.S. 1985, c. P-21;

"Record" means any hard copy document or any data in a machine-readable format containing Personal Information;

ii. Words and expressions defined in the General Conditions and used in these supplemental general conditions have the meanings given to them in the General Conditions.

iii. If there is any inconsistency between the General Conditions and these supplemental general conditions, the applicable provisions of these supplemental general conditions prevail.

(e) **Ownership of Personal Information and Record**

To perform the Work, the foreign recipient **Contractor / Subcontractor** will be provided with and/or will be collecting Personal Information from third parties. The foreign recipient **Contractor / Subcontractor** acknowledges that it has no rights in the Personal Information or the Records and that Canada owns the Records. On request, the foreign recipient **Contractor / Subcontractor** must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

(f) **Use of Personal Information**

The foreign recipient **Contractor / Subcontractor** agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Work in accordance with the **contract / subcontract**.

(g) **Collection of Personal Information**

(i) If the foreign recipient **Contractor / Subcontractor** must collect Personal Information from a third party to perform the Work, the foreign recipient **Contractor / Subcontractor** must only collect Personal Information that is required to perform the Work. The foreign recipient **Contractor / Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor / Subcontractor** must inform that individual (at or before the time when it collects the Personal Information) of the following:

i. that the Personal Information is being collected on behalf of, and will be provided to, Canada;

ii. the ways the Personal Information will be used;

iii. that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;

iv. the consequences, if any, of refusing to provide the information;

v. that the individual has a right to access and correct his or her own Personal Information; and

vi. that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the foreign recipient **Contractor / Subcontractor**.

(ii) The foreign recipient Contractor, its subcontractors, and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

(iii) If requested by the Contracting Authority, the foreign recipient **Contractor / Subcontractor** must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The foreign recipient **Contractor / Subcontractor** must not begin using the form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.

(iv) At the time it requests Personal Information from any individual, if the foreign recipient **Contractor / Subcontractor** doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the foreign recipient **Contractor / Subcontractor** must ask the Contracting Security Authority for instructions.

(h) **Maintaining the Accuracy, Privacy and Integrity of Personal Information**

The foreign recipient **Contractor / Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient **Contractor / Subcontractor** must protect the privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor / Subcontractor** must:

(i) not use any personal identifiers (e.g. social insurance number) to link multiple databases containing Personal Information;

(ii) segregate all Records from the foreign recipient **Contractor's/Subcontractor's** own information and records;

(iii) restrict access to the Personal Information and the Records to people who require access to perform the Work (for example, by using passwords or biometric access controls);

(iv) provide training to anyone to whom the foreign recipient **Contractor / Subcontractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Work. The foreign recipient **Contractor / Subcontractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor / Subcontractor** must keep a record of the training and make it available to the Contracting Authority if requested;

(v) if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the foreign recipient **Contractor / Subcontractor** provides access to the Personal Information to acknowledge in writing

(in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;

(vi) keep a record of all requests made by an individual to review his or her Personal Information, and any requests to correct errors or omissions in the Personal Information (whether those requests are made directly by an individual or by Canada on behalf of an individual);

(vii) include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor / Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor / Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

(viii) keep a record of the date and source of the last update to each Record;

(ix) maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the foreign recipient **Contractor / Subcontractor** and Canada at any time; and

(x) secure and control access to any hard copy Records.

(i) **Safeguarding Personal Information**

The foreign recipient **Contractor / Subcontractor** must safeguard the Personal Information at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality. To do so, at a minimum, the foreign recipient **Contractor / Subcontractor** must:

(i) store the Personal Information electronically so that a password (or a similar access control mechanism, such as biometric access) is required to access the system or database in which the Personal Information is stored;

(ii) ensure that passwords or other access controls are provided only to individuals who require access to the Personal Information to perform the Work;

(iii) not outsource the electronic storage of Personal Information to a third party (including an affiliate) unless the Canadian DSA has first consented in writing;

(iv) safeguard any database or computer system on which the Personal Information is stored from external access using methods that are generally used, from time to time, by prudent public and private sector organizations in Canada in order to protect highly secure or sensitive information;

(v) maintain a secure back-up copy of all Records, updated at least weekly;

(vi) implement any reasonable security or protection measures requested by Canada from time to time; and

(vii) notify the Contracting Authority and the Canadian DSA immediately of any security breaches; for example, any time an unauthorized individual accesses any Personal Information.

(j) **Appointment of Privacy Officer**

The foreign recipient **Contractor / Subcontractor** must appoint someone to be its privacy officer and to act as its representative for all matters related to the Personal Information and the Records. The foreign recipient **Contractor / Subcontractor** must provide that person's name to the Contracting Authority and the Canadian DSA within ten (10) days of the award of the **Contract / subcontract**.

(k) **Quarterly Reporting Obligations**

Within 30 calendar days of the end of each quarter (January-March; April-June; July-September; October-December), the foreign recipient **Contractor / Subcontractor** must submit the following to the Contracting Authority:

(i) a description of any new measures taken by the foreign recipient **Contractor / Subcontractor** to protect the Personal Information (for example, new software or access controls being used by the foreign recipient **Contractor / Subcontractor**);

(ii) a list of any corrections made to Personal Information at the request of an individual (including the name of the individual, the date of the request, and the correction made);

(iii) details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the **Contractor / Subcontractor**; and

(iv) a complete copy (in an electronic format agreed to by the Contracting Authority and the foreign recipient **Contractor / Subcontractor**) of all the Personal Information stored electronically by the **contract / subcontract**.

(l) **Threat and Risk Assessment**

Within ninety (90) calendar days of the award of the **contract / subcontract** and, if the **contract/ subcontract** lasts longer than one year, within thirty (30) calendar days of each anniversary date of the **contract / subcontract**, the foreign recipient **Contractor / Subcontractor** must submit to the Contracting Authority and the Canadian DSA a threat and risk assessment, which must include:

(i) a copy of the current version of any request for consent form or script being used by the foreign recipient **Contractor / Subcontractor** to collect Personal Information;

(ii) a list of the types of Personal Information used by the foreign recipient **Contractor / Subcontractor** in connection with the Work;

(iii) a list of all locations where hard copies of Personal Information are stored;

(iv) a list of all locations where Personal Information in machine-readable format is stored (for example, the location where any server housing a database including any Personal Information is located), including back-ups;

(v) a list of every person to whom the foreign recipient **Contractor / Subcontractor** has granted access to the Personal Information or the Records;

(vi) a list of all measures being taken by the foreign recipient **Contractor / Subcontractor** to protect the Personal Information and the Records;

(vii) a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and

(viii) an explanation of any new measures the foreign recipient **Contractor / Subcontractor** intends to implement to safeguard the Personal Information and the Records.

(m) **Audit**

Canada may audit the foreign recipient **Contractor's/Subcontractor's** compliance with these supplemental general conditions at any time. If requested by the Contracting Authority, the foreign recipient **Contractor / Subcontractor** must provide Canada (or Canada's authorized representative) with access to its premises and to the Personal Information and Records at all reasonable times. If Canada identifies any deficiencies during an audit, the foreign recipient **Contractor / Subcontractor** must immediately correct the deficiencies at its own expense.

(n) **Statutory Obligations**

(i) The foreign recipient **Contractor / Subcontractor** acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's *Privacy Act*, *Access to Information Act*, R.S. 1985, c. A-1, and *Library and Archives of Canada Act*, S.C. 2004, c. 11. The foreign recipient **Contractor / Subcontractor** agrees to comply with any requirement established by the Contracting Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

(ii) The foreign recipient **Contractor / Subcontractor** acknowledges that its obligations under the **contract / subcontract** are in addition to any obligations it has under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, or similar legislation in effect from time to time in any province or territory of Canada. If the foreign recipient **Contractor / Subcontractor** believes that any obligations in the **contract / subcontract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor / Subcontractor** must immediately notify the Contracting Authority of the specific provision of the **contract / subcontract** and the specific obligation under the law with which the foreign recipient **Contractor / Subcontractor** believes it conflicts.

(o) **Disposing of Records and Returning Records to Canada**

The foreign recipient **Contractor / Subcontractor** must not dispose of any Record, except as instructed by the Contracting Authority. On request by the Contracting Authority, or once the Work involving the Personal Information is complete, the **contract / subcontract** is complete, or the **contract / subcontract** is terminated, whichever of these comes first, the foreign recipient **Contractor / Subcontractor** must return all Records (including all copies) to the Contracting Authority.

(p) **Legal Requirement to Disclose Personal Information**

Before disclosing any of the Personal Information pursuant to any applicable legislation, regulation, or an order of any court, tribunal or administrative body with jurisdiction, the foreign recipient **Contractor / Subcontractor** must immediately notify the Contracting Authority, in order to provide the Contracting Authority with an opportunity to participate in any relevant proceedings.

(q) **Complaints**

Canada and the foreign recipient **Contractor / Subcontractor** each agree to notify the other immediately if a complaint is received under the *Access to Information Act* or the *Privacy Act* or other relevant legislation regarding the Personal Information. Each Party agrees to provide

any necessary information to the other to assist in responding to the complaint and to inform the other immediately of the outcome of that complaint.

(r) **Exception**

The obligations set out in these supplemental general conditions do not apply to any Personal Information that is already in the public domain, as long as it did not become part of the public domain as a result of any act or omission of the Contractor or any of its subcontractors, agents, or representatives, or any of their employees.

7.19 Contractor's Sites or Premises Requiring Safeguarding Measures

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

Street Number / Street Name, Unit / Suite / Apartment Number

City, Province, Territory / State

Postal Code / Zip Code

Country

The Company Security Officer must ensure through the Contract Security Program that the Contractor and individuals hold a valid security clearance at the required level of document safeguarding capability.

7.20 Physical and Information Security

The Government of Canada has security requirements that any informatics system must meet in order to protect Canadian personal information, privacy and/or governmental assets. The Contractor must implement security measures that will protect the system that is deemed to store unclassified information, with low integrity and availability. The Contractor must deliver access to and use of a Solution that will protect Canadian citizens, and Government of Canada information and assets by implementing security controls, measures and/or devices within the Solution.

7.21 Basis of Payment

(a) **Phase 1 – Prototype Solution:** For the Work described in Phase 1 – Prototype Solution of Annex A – Statement of Work. In consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid an all-inclusive firm lot price in accordance with Annex B – Basis of Payment, in Canadian funds, customs duty included, Goods and Services Tax or Harmonized Sales Tax is extra, if applicable. The all-inclusive firm lot price includes the delivery of a Prototype Solution. This delivery includes the usage rights, grants and access, training of users, the software documentation, warranty, and maintenance and support, waivers, non-disclosure agreements and other releases to Canada for the purposes of conducting the Capability and Usability Assessment (CUA). The price includes up to 100 User Licenses or Accesses or both, as applicable, to use the Prototype Solution for Capability and Usability Assessment purposes during the initial contract.

(b) **Phase 1- Prototype on Platform (PoP) Test (if applicable):** As may be requested by the Contracting Authority for Work described to conduct the Prototype on Platform (PoP) test. In consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid an all-inclusive firm lot price in accordance with Annex B – Basis of Payment, in Canadian funds, customs duty included, Goods and Services Tax or Harmonized

Sales Tax is extra, if applicable. The all-inclusive firm lot price includes the installation and integration of the Prototype Solution on RCMP's Protected B cloud tenant, usage rights, grants and access, Software Documentation, Warranty, Maintenance and Support, waivers, non-disclosure agreements and other releases to Canada for purposes of conducting the PoP test for up to 100 User Licenses or Accesses or both, as applicable, to use the Prototype Solution.

(c) **Optional Phase 2 – Solution:** At Canada's sole discretion, Canada may exercise the irrevocable option to deliver the full Solution in accordance with Phase 2 - Solution of Annex A – Statement of Work. If Canada exercises this irrevocable option, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid an all-inclusive firm lot price(s) in accordance with Annex B – Basis of Payment, in Canadian funds, customs duty included, Goods and Services Tax or Harmonized Sales Tax is extra, if applicable. The all-inclusive firm lot price includes, whenever applicable to the proposed Solution delivery model, the delivery, installation, integration and configuration of the Solution, incidental and additionally required information technology infrastructure services, Software Documentation, Warranty, Maintenance and Support, Training during Solution implementation period, waivers, non-disclosure agreements, other releases to Canada and all User Licenses and Accesses or both, as applicable, for up to 2000 users to access and use the Solution in accordance with the Contract.

(d) **Optional Additional User Licenses or Additional User Accesses or both, as applicable:** At Canada's sole discretion, may exercise the irrevocable option for the Contractor to deliver Additional User Licenses or Additional User Accesses or both, as applicable. If Canada exercises this irrevocable option, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a firm lot price(s) in accordance with Annex B – Basis of Payment, in Canadian funds, customs duty included, Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

(e) **Optional Professional Services provided under a Task Authorization with a Firm Price**: For professional services requested by Canada, in accordance with a validly issued Task Authorization and the Contractor satisfactorily completing its obligations under the Contract, Canada will pay the Contractor the firm price (travel and living expenses excluded), as set out in the Task Authorization, applicable Taxes extra in accordance with the firm per diem rates set out in Annex B, Basis of Payment. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday.

(f) **Optional Training Services provided under a Task Authorization with a Firm Price:** For training services requested by Canada, in accordance with a validly issued Task Authorization and the Contractor satisfactorily completing its obligations under the Contract, Canada will pay the Contractor the firm price (travel and living expenses excluded), as set out in the Task Authorization, Applicable Taxes extra in accordance with the firm lot price set out in Annex B, Basis of Payment.

(g) **Optional Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both (if applicable) provided under a Task Authorization with a Firm Price**: For Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both (if applicable) requested by Canada, in accordance with a validly issued Task Authorization and the Contractor satisfactorily completing its obligations under the Contract, Canada will pay the Contractor the firm price per Deliverable as set out in the Task Authorization, Applicable Taxes extra in accordance with the firm lot prices set out in Annex B, Basis of Payment. Partial period

of support services will be prorated based on actual period year supplied based on a 365-day per year.

(h) **Travel and Living Expenses – National Joint Council Travel Directive**: The Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal, and private vehicle allowances specified in Appendices B, C and D of the National Joint Council Travel Directive, and with the other provisions of the directive referring to "travellers", rather than those referring to "employees". Canada will not pay the Contractor any incidental expense allowance for authorized travel.

(i) All travel must have the prior authorization of the Technical Authority.

(ii) All payments are subject to government audit.

(i) **Limitation of Price.** 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.

(j) **Limitation of Expenditure – Professional Services provided under a Task Authorization**

(i) Canada's total liability to the Contractor under the Contract for all authorized Task Authorizations (Task), inclusive of any revisions, must not exceed the sum of $_____ *(to be inserted at contract award).* Customs duties are included and Applicable Taxes are extra.

(ii) No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

(iii) The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

(1) when it is 75 percent committed, or
(2) four (4) months before the contract expiry date, or
(3) as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized Task, inclusive of any revisions,
whichever comes first.

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

(k) **Limitation of Expenditure – Training provided under a Task Authorization**

(i) Canada's total liability to the Contractor under the Contract for all authorized Task Authorizations (Task), inclusive of any revisions, must not exceed the sum of $_____ *(to be inserted at contract award).* Customs duties are included and Applicable Taxes are extra.

(ii) No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

(iii) The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

i. when it is 75 percent committed, or

ii. four (4) months before the contract expiry date, or

iii. as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized Task, inclusive of any revisions, whichever comes first.

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

(l) **Limitation of Expenditure – Optional Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both (if applicable), provided under a Task Authorization**

(i) Canada's total liability to the Contractor under the Contract for all authorized Task Authorizations (Task), inclusive of any revisions, must not exceed the sum of $_____ *(to be inserted at contract award).* Customs duties are included and Applicable Taxes are extra.

(ii) No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

(iii) The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

(1) when it is 75 percent committed, or
(2) four (4) months before the contract expiry date, or
(3) as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized Task, inclusive of any revisions, whichever comes first.

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

7.22 Method of Payment

(a) **Single Payment – Phase 1 – Prototype Solution** (Ref. Table 1 of Annex B, Basis of Payment)

Canada will pay the Contractor upon completion and delivery of the Work under Phase 1- Prototype solution in accordance with the payment provisions of the Contract if:

(i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
(ii) all such documents have been verified by Canada;
(iii) the Work delivered has been accepted by Canada.

(b) **Single Payment – Phase 1 – PoP Test, if applicable** (Ref. Table 2 of Annex B, Basis of Payment)

Canada will pay the Contractor upon completion and delivery of the Work under Phase 1 - PoP Test in accordance with the payment provisions of the Contract if:

(iv) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
(v) all such documents have been verified by Canada; and
(vi) the Work delivered has been accepted by Canada.

(c) **Optional Phase 2- Milestone Payments, Subject to holdback- Implementation of Solution** (Ref. Table 3 and Table Schedule of Milestone Payments Implementation Support of Annex B, Basis of Payment)

At Canada's sole discretion, Canada may exercise the irrevocable option for the Contractor to perform Work in accordance with article 3. Phase 2 - Solution of Annex A – Statement of Work. If Canada exercises this irrevocable option, Canada will make milestone payments to the Contractor in accordance with the Schedule of Milestones detailed in Annex B -Basis of Payment and the payment provisions of the Contract, up to 90% percent of the amount claimed and approved by Canada if:

(i) an accurate and complete claim for payment using form PWGSC-TPSGC 1111, Claim for Progress Payment, and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
(ii) the total amount for all milestone payments paid by Canada does not exceed 90% percent of the total amount to be paid under the Contract;
(iii) all the certificates appearing on form PWGSC-TPSGC 1111 have been signed by the respective authorized representatives;
(iv) all work associated with the milestone and as applicable any deliverable required have been completed and accepted by Canada.

The balance of the amount payable will be paid in accordance with the payment provisions of the Contract upon completion and delivery of all Work required under the Contract if the Work has been accepted by Canada and a final claim for the payment is submitted.

(d) **Monthly Payment – Optional Additional User Licenses or Additional User Accesses or both, as applicable** (Ref. Table 4, Table 5A, Table 5B of Annex B, Basis of Payment)

At Canada's sole discretion, Canada may exercise the irrevocable option for the Contractor to deliver Additional User Licenses or Additional User Accesses or both, as applicable. If Canada exercises this irrevocable option, Canada will pay the Contractor on a monthly basis for additional User Licenses or additional User Accesses or both, as applicable obtained during the month covered by the invoice in accordance with the payment provisions of the Contract if:

(i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
(ii) all such documents have been verified by Canada; and
(iii) the Work performed has been accepted by Canada.

(e) **Monthly Payment – Task Authorized Optional Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if**

applicable) or both (if applicable) with a Firm Price (Ref. Table 6 of Annex B, Basis of Payment)

At Canada's sole discretion, Canada may exercise the irrevocable option for the Contractor to deliver Solution Maintenance and Support Services (if applicable) or NCS Hosting and Hosting Related Support Services (if applicable) or both if applicable. If Canada exercises this irrevocable option, Canada will pay the Contractor on a monthly basis for Optional Solution Maintenance and Support Services or NCS Hosting and Hosting Related Support Services or both, as applicable obtained during the month covered by the invoice in accordance with the payment provisions of the Contract if:

(i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
(ii) all such documents have been verified by Canada; and
(iii) the Work performed has been accepted by Canada.

(f) **Monthly Payment – Task Authorized Optional Professional Services with a Firm Price** (Ref. Table 7 of Annex B, Basis of Payment)

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

(i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
(ii) all such documents have been verified by Canada; and
(iii) the Work performed has been accepted by Canada.

(g) **Monthly Payment – Task Authorized Optional Training Services with a Firm Price** (Ref. Table 8 of Annex B, Basis of Payment)

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

(i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
(ii) all such documents have been verified by Canada; and
(iii) the Work performed has been accepted by Canada.

7.23 Invoicing

(a) **Invoice Submission**. The Contractor must submit invoices for the Services and delivery of any Work, as applicable.

(b) **Invoice Requirements**. Invoices must be submitted in the Contractor's name and contain:

(i) the date, the name and address of the client department, item or reference numbers, deliverable/description of the Work, contract number, Client Reference Number (CRN), Procurement Business Number (PBN), and financial code(s);

(ii) details of expenditures (such as item, quantity, unit of issue, unit price, fixed time labour rates and level of effort, subcontracts, as applicable) in accordance with the Basis of Payment, exclusive of Applicable Taxes;

(iii) deduction for holdback, if applicable; and the extension of the totals, if applicable.

Applicable Taxes must be shown as a separate line item along with corresponding registration numbers from the tax authorities and all items that are zero-rated, exempt or to which Applicable Taxes do not apply, must be identified as such on all invoices.

(c) **Invoicing Instructions – Release of Holdback and Balance of Amount Payable**

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

In addition to the requirements of the general conditions, each invoice must be supported by:

i. All applicable release documents as well as any other documents called for under the Contract; and

ii. All Certificate(s) of Inspection pertaining to the goods and / or services which are the subject of the invoice, provided as a scanned PDF copy with official signatures of the designated certification authorities and not just printed names.

(ii) As per Contract Article on milestone payments any balance of the amount payable will be paid in accordance with the payment provisions of the Contract, upon completion and delivery of all work required under each task authorization of the Contract, and upon completion of any adjustment required as described under the "Basis of Payment" if the Work has been accepted by Canada and a final invoice for payment is submitted.

(iii) Invoices must be distributed as follows:

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

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

7.24 Taxes

(a) **Payment of Taxes.** Applicable Taxes will be paid by Canada as provided in the Invoice Submission section. It is the sole responsibility of the Contractor to charge Applicable Taxes at the correct rate in accordance with applicable legislation. The Contractor must remit to appropriate tax authorities any amounts of Applicable Taxes paid or due.

(b) **Withholding for Non-Residents.** Canada must withhold 15 percent of the amount to be paid to the Contractor in respect of services provided in Canada if the Contractor is not a resident of Canada, unless the Contractor obtains a valid waiver from the Canada Revenue Agency. The amount withheld will be held on account for the Contractor in respect to any tax liability which may be owed to Canada.

(c) **Foreign-based Contractor.** Unless specified otherwise in the Contract, the price includes no amount for any federal excise tax, state or local sales or use tax, or any other tax of a similar nature, or any Canadian tax whatsoever. The price, however, includes all other taxes. If the Work is normally subject to federal excise tax, Canada will, upon request, provide the Contractor a

certificate of exemption from such federal excise tax in the form prescribed by the federal regulations.

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

(e) **Certification of Invoices.** By submitting an invoice, the Contractor certifies that the invoice is consistent with the Work delivered and is in accordance with the Contract.

(f) **Payment Period.** Canada will pay the Contractor's undisputed invoice amount within 30 days of receipt. In the event, an invoice is not in acceptable form and content, Canada will notify the Contractor and the 30 day payment period will begin on receipt of a conforming invoice.

(g) **Interest on Late Payments.** Canada will pay to the Contractor simple interest at the Average Rate plus 3 percent per year on any amount that is overdue, from the date that amount becomes overdue until the day before the date of payment, inclusive, provided Canada is responsible for the delay in paying the Contractor. Canada will not pay interest on overdue advance payments.

(h) Electronic Payment of Invoices – Contract

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

(i) Visa Acquisition Card:

(ii) MasterCard Acquisition Card;

(iii) Direct Deposit (Domestic and International);

(iv) Electronic Data Interchange (EDI);

(v) Wire Transfer (International Only);

(vi) Large Value Transfer System (LVTS) (Over $25M)

7.25 Certifications and Additional Information

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

7.26 Federal Contractors Program for Employment Equity – Default by 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.

7.27 Insurance Requirements

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

7.28 Price Certification

The Contractor certifies that the price quoted is not in excess of the lowest price charged anyone else, including the Contractor's most favoured customer, for the like quality and quantity of the goods, services or both.

7.29 Limitation of Liability

Except as expressly provided in paragraph (b), the Contractor is liable to Canada for all direct damages it causes in performing or failing to perform the Contract in relation to:

(a) The Contractor's acts or omissions under the Contract affecting real or tangible personal property owned, possessed or occupied by Canada;

(b) The Contractor's breach of confidentiality obligations under the Contract, but such limitation does not apply to the disclosure by Contractor of the trade secrets of Canada or a third party related to information technology;

(c) Liens or encumbrances relating to any portion of the Work under the Contract, not including claims or encumbrances relating to intellectual property rights; and

(d) Contractors breach of warranty obligations.

However, the Contractor is not liable to Canada for indirect, special or consequential damages caused by items (a) to (d) above.

With respect to direct damages related to the Contractor's breach of warranty obligations, the Contractor's maximum liability to Canada is the total estimated cost of the Contract (meaning the dollar amount shown on the first page of the Contract in the block titled "**Total Estimated Cost**"). All direct damages not listed above that do not relate to breach of warranty are subject to a maximum of .25 times the Total Estimated Cost or $1M, whichever is greater.

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.

None of the above limitations apply to damages based on loss of life or injury or claims based on infringement of intellectual property.

7.30 General Provisions

(a) **Applicable Laws**. This Contract will be interpreted and governed by the laws of Ontario.

(b) **Survival**. All the parties' obligations of confidentiality, representations and warranties set out in the Contract as well as the provisions, which by the nature of the rights or obligations might reasonably be expected to survive, will survive the expiry or termination of the Contract.

(c) **Severability**. If any provision of this Contract is declared unenforceable by an authoritative court, the remainder of this Contract will remain in force.

(d) **Waiver**. The failure or neglect by a party to enforce any of rights under this Contract will not be deemed to be a waiver of that party's rights.

(e) **No Bribe**. The Contractor warrants that no bribe, gift, benefit, or other inducement has been or will be paid, given, promised or offered directly or indirectly to any official or employee of Canada or to a member of the family of such a person, with a view to influencing the entry into the Contract or the administration of the Contract.

(f) **Contingency Fees**. The Contractor represents that it has not, directly or indirectly, paid or agreed to pay and agrees that it will not, directly or indirectly, pay a contingency fee for the solicitation, negotiation or obtaining of the Contract to any person, other than an employee of the Contractor acting in the normal course of the employee's duties. In this section, "contingency fee" means any payment or other compensation that depends or is calculated based on a degree of success in soliciting, negotiating or obtaining the Contract and "person" includes any individual who is required to file a return with the registrar pursuant to section 5 of the *Lobbying Act*, 1985, c. 44 (4th Supplement).

(g) **International Sanctions**.

(i) Persons in Canada, and Canadians outside of Canada, are bound by economic sanctions imposed by Canada. As a result, the Government of Canada cannot accept delivery of goods or services that originate, either directly or indirectly, from the countries or persons subject to economic sanctions.

(ii) The Contractor must not supply to the Government of Canada any goods or services which are subject to economic sanctions.

The Contractor must comply with changes to the regulations imposed during the period of the Contract. The Contractor must immediately advise Canada if it is unable to perform the Work as a result of the imposition of economic sanctions against a country or person or the addition of a good or service to the list of sanctioned goods or services. If the Parties cannot agree on a work around plan, the Contract will be terminated.

(h) **Integrity Provisions – Contract**. The *Ineligibility and Suspension Policy* (the "Policy") and all related Directives incorporated by reference into the bid solicitation on its closing date are incorporated into, and form a binding part of the Contract. The Contractor must comply with the provisions of the Policy and Directives, which can be found on Public Services and Procurement Canada's website at *Ineligibility and Suspension Policy*.

(i) **Code of Conduct for Procurement – Contract**. The Contractor agrees to comply with the *Code of Conduct for Procurement* and to be bound by its terms for the period of the Contract.

(j) **Conflict of interest and Values and Ethics Codes for the Public Service**. The Contractor acknowledges that individuals who are subject to the provisions of the *Conflict of interest Act*, 2006, c. 9, s. 2, the Conflict of interest Code for Members of the House of Commons, the Values and Ethics Code for the Public Service or all other codes of values and ethics applicable within specific organizations cannot derive any direct benefit resulting from the Contract.

7.31 Authorities

(a) **Contracting Authority**

The Contracting Authority for the Contract is:

Name:	**Jean-Claude Labossière**
Title:	Supply Specialist
Organization:	Public Services and Procurement Canada, Acquisitions Branch
Directorate:	Applications and Software Procurement Directorate
Address:	10 Rue Wellington, Gatineau, QC K1A 0S5
Telephone:	613-858-7359
E-mail address:	jean-claude.labossiere@tpsgc-pwgsc.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.

(b) Technical Authority – Royal Canadian Mounted Police

Will be added at Contract Award.

Name:	_____
Title:	_____
Organization:	_____
Address:	_____
Telephone:	_____
Facsimile:	_____
E-mail address:	_____

The Technical Authority [is the representative of the department or agency for whom the Work is being carried out under the Contract and] is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

(c) Supply Chain Security Authority (Will be added at Contract Award).

Name:

Title:

Phone:

E-mail address:

The Supply Chain Security Authority is the SSC representative and is responsible for all matters concerning the ongoing Supply Chain Integrity Process under the Contract. Neither the Contracting Authority nor the Technical Authority have any authority to advise or authorize any

information in relation to the Supply Chain Integrity Process. All other security-related matters remain the responsibility of the Supply Chain Security Authority.

7.32 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a Public Service Superannuation Act (PSSA) pension, the Contractor has agreed that this information will be reported on departmental web sites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

7.33 Priority of Documents

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

(a) these Articles of Agreement, including any individual SACC Manual clauses incorporated by reference in these Articles of Agreement;

(b) the general conditions 2035 (2020-05-28) General Conditions – Higher Complexity – Services

(c) the general conditions 2030 (2020-05-28), General Conditions - Higher Complexity - Goods

(d) the supplemental general conditions, in the following order:

(i) 4008, (2008-12-12) Personal Information

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

(iii) 4003 (2010-08-16), Supplemental General Conditions - Licensed Software

(iv) 4004 (2013-04-25), Supplemental General Conditions - Maintenance and Support Services for Licensed Software

(e) Annex A – Statement of Work

(f) Annex B – Basis of Payment

(g) Annex C – Security Requirement Check List

(h) Annex D – Definitions and Interpretations

(i) Annex E – Privacy Obligations

(j) Annex F – Supply Chain Integrity

(k) the signed Task Authorizations and any Certifications as required;

(l) Annex G – Task Authorization Forms

(m) Annex H – Progress Claims

(n) Annex I – Bidder Forms

(o) the Contractor's bid dated _____ (*insert date of bid)*

7.34 Foreign National (Canadian Contractor)

(a) SACC Manual clause A2000C (2006-06-16) Foreign Nationals (Canadian Contractor)

Note to Bidders: Either this clause or the one that follows, whichever applies (based on whether the successful Bidder is a Canadian Contractor or Foreign Contractor), will be included in any resulting contract.

7.35 Foreign National (Foreign Contractor)

SACC Manual clause A2001C (2006-06-16) Foreign Nationals (Foreign Contractor).

7.36 Joint Venture Contractor

(a) The Contractor confirms that the name of the joint venture is _____ and that it is comprised of the following members:

(b) With respect to the relationship among the members of the joint venture Contractor, each member agrees, represents and warrants (as applicable) that:

(i) _____ has been appointed as the "representative member" of the joint venture Contractor and has full authority to act as agent for each member regarding all matters relating to the Contract;

(ii) by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Contractor; and

(iii) all payments made by Canada to the representative member will act as a release by all the members.

(c) All the members agree that Canada may terminate the Contract in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.

(d) All the members are jointly and severally or solidarily liable for the performance of the entire Contract.

(e) The Contractor acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.

(f) The Contractor acknowledges that all security and controlled goods requirements in the Contract, if any, apply to each member of the joint venture Contractor.

Note to Bidders: *This Article will be deleted if the Bidder awarded the contract is not a joint venture. If the contractor is a joint venture, this clause will be completed with information provided in its bid.*

BID SOLICITATION

ANNEXES

NATIONAL CYBERCRIME SOLUTION
FOR
CANADA ROYAL CANADIAN MOUNTED POLICE

Table of Contents

THIS PAGE IS PURPOSELY BLANK

ANNEX A

STATEMENT OF WORK

NATIONAL CYBERCRIME SOLUTION

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Introduction

1.1 Title

a) National Cybercrime Solution (NCS), referred to hereafter as the “Solution.”

1.2 Background

a) In 2015, the Prime Minister of Canada asked the Minister of Public Safety and Emergency Preparedness to lead, “a review of existing measures to protect Canadians and our critical infrastructure from cyber threats,” (the Cyber Review). The Cyber Review consisted of public and stakeholder consultations in 2016 and an interdepartmental policy development process in 2016 and 2017. The Cyber Review concluded that Canada needs a national mechanism to coordinate police operations against cybercriminals as well as a national mechanism for Canadians and businesses to report cybercrimes to police (among other initiatives).

b) Police in Canada and elsewhere encounter similar cybercrimes and this similarity in international criminal activity calls for domestic and multilateral coordination. However, the Canadian policing community needs a national cybercrime coordination organization that is enabled by a robust cybercrime-specific Information Management / Information Technology (IM/IT) system to connect the dots, coordinate Canadian investigative efforts domestically and internationally, and assess the wider economic and social impacts of cybercrime. Not addressing this need results in missed investigative opportunities and risks as well as a duplication of efforts.

c) Crime reporting is fundamental to investigations, to protecting victims, and to understanding and preventing crime. This activity applies equally to cybercrime and fraud. Traditional frauds are increasingly being enabled by digital technologies (‘old crimes in new ways’), and the lines between a traditional fraud and a cybercrime are often not clear. Whereas victims of traditional localized crimes may report such activity to local police, the how-to of reporting cybercrimes is less clear and this obscurity results in confusion for the public.

d) Currently, there is no single national system that provides Canadians and businesses with an easy-to-use means to report cybercrimes to police or one that gives police agencies access to victim reports and analytics. Not addressing this need hampers investigations, macro analysis, threat identification, and a coordinated police effort to understand and respond to cybercrime. In order to improve public reporting, the Royal Canadian Mounted Police (RCMP) will build a system that will receive reports for both cybercrime and fraud.

e) These key gaps—a lack of cybercrime coordination organization and a lack of a national cybercrime public reporting mechanism—were raised by numerous law enforcement and other respondents during the Cyber Review consultations. In response, the RCMP established the National Cybercrime Coordination Unit (NC3) which will be enabled by the new cybercrime-specific Solution.

1.3 Overview

a) The mandate of NC3 is to enable Canadian law enforcement to reduce the threat, victimization, and impact of cybercrime on Canadians.

b) The NC3 will:

i) Coordinate Canadian law enforcement cybercrime operations and collaborate with international partners;

ii) Provide digital investigative advice and guidance to Canadian police;

iii) Produce actionable cybercrime intelligence;

iv) Establish a national public reporting mechanism for Canadians and businesses to report cybercrimes and frauds to law enforcement;

v) Share cybercrime information with police agencies;

vi) Search for linkages among distinct cyber events; and

vii) Help to ensure that multiple police agencies are not duplicating efforts by investigating the same crime or suspect separately.

1.4 Objectives

a) NC3 requires an advanced, leading edge National Cybercrime Solution to fulfil its mandate.

b) The Solution must:

i) Enable and support secure two-way exchange of cybercrime requests and information with law enforcement Partners (including but not limited to domestic, international law enforcement and federal agencies) via a Police and Partner Portal (P3) as well as other traditional means including but not limited to email;

ii) Support the exchange of large volumes of structured, semi-structured, and unstructured data;

iii) Provide capabilities as documented in Appendix C – NCS Business Capability Model;

iv) Provide case management capabilities including receipt, capture, analysis, enrichment, correlation, assessment and deconfliction of information, and integration within the Solution to create new investigations or to further existing investigations;

v) Provide capabilities to deconflict and coordinate cybercrime and fraud intelligence efforts across the Canadian law enforcement community as well as with federal and international organizations;

vi) Provide Users with the capability to analyze data in order to generate intelligence and to support decision making;

vii) Provide data visualization to support conclusions and inferences;

viii) Provide advanced data mining features to support NC3 Users with the analysis of unstructured, semi-structured, and structured data;

ix) Provide cybercrime partners with investigative and technical advice, tools, and guidance and do so directly and through an online knowledge base using the P3;

x) Facilitate the identification of malware samples from the Canadian law enforcement community against selected domestic or international malware libraries in order to support intelligence and investigation efforts; and

xi) Provide capabilities to actively manage engagements and partnerships with the Private Sector and other Government Departments.

c) Work will be conducted in accordance with the two (2) Phases described below. The Contractor must under Phase 1 work to develop and deliver a Prototype Solution within a stipulated period in accordance with Phase 1 work described in Annex A - Statement of Work and the Capability and Usability Assessment (CUA) criteria in Appendix A to Annex A-Statement of Work. On completion of Phase 1 work and an assessment of the Prototype Solutions by Canada, Canada will at its sole discretion exercise the irrevocable option for the Contractor to work and deliver the full Solution in accordance with Phase 2 of Annex A – Statement of Work.

1.5 Out of Scope

a) The RCMP is developing a Public Reporting Website. The development of this website is out-of-scope of this SOW. Details on the Public Reporting Website are included in this SOW to provide the Contractor with context related to a primary feed of Cybercrime Reports to the Solution.

b) The RCMP acts as a broker only with respect to malware cross-reference requests and does not perform detailed malware analysis; therefore, malware analysis is not within the scope of the Solution.

2. Phase 1 – Prototype Solution

2.1 Scope of Work

a) The scope of work for the Prototype Solution involves the planning, design, development, configuration, testing, and delivery of a production quality, hosted, Cloud based, working Prototype Solution supporting up to one-hundred (100) Users in accordance with the technical and functional requirements described herein.

2.2 Requirements

a) The Contractor must develop and deliver a cloud based Prototype Solution that may be comprised of any combination of Commercial-Off-The-Shelf (COTS) software, custom or open-source software in accordance with the requirements described in this section and in Appendix A – Capability and Usability Assessment (CUA). Interoperability and Integration points between components of the Prototype Solution must be transparent to the User.

b) The Contractor's resulting configuration of the Prototype Solution must provide Canada with an integrated application that supports all capabilities and requirements described in the user scenarios detailed in Appendix A – Capability and Usability Assessment (CUA) specifically:

   i) User Scenario No. 1 – Partner Service Request;

   ii) User Scenario No. 2 – Municipal Ransomware – Coordinate and Assist;

   iii) User Scenario No. 3 – Partner Requests Digital Advice and Guidance;

   iv) User Scenario No. 4 – Analytics; and

   v) User Scenario No. 5 – Public Report Integration.

c) Further details on the content of each scenario are described in Appendix A – Capability and Usability Assessment (CUA).

2.3 Prototype Security

a) In the event of a security breach that impacts Prototype security, or has the potential to compromise Canada or its clients in any other level of government, the Contractor must inform Canada that a security breach has occurred. Canada will identify the time frame in which the risk must be addressed in the associated Vulnerability Mitigation Report.

b) The Contractor must retain any security violations, transactions, audit records, and alarm incident records and associated reports for the current and previous three (3) years and must obtain Canada's written permission to destroy any records after two (2) years.

c) The Contractor must provide Security Audit Log records to Canada within ten (10) working days of a request by Canada.

2.4 Capability and Usability Assessment

Canada will conduct a Capability and Usability Assessment (CUA) of the Prototype Solution deliverables in accordance with the assessment procedures and criteria defined in assessment procedures and criteria

a) defined in Appendix A – Capability and Usability Assessment (CUA).

2.5 Prototype on Platform (POP) Test

Canada may conduct, at its sole discretion, a Prototype on Platform (POP) Test using the Prototype Solution proposed by the top-ranked Contractor (identified after the CUA).

a) If the Solution is delivered on the RCMP Protected B Cloud or using a Hybrid model, the POP test will be used to confirm that the Prototype Solution operating in the Contractor's Cloud Tenant can be installed and deployed per the proposed Solution Architecture and Cloud Service Delivery Model (CSDM).

   i) The POP Test must demonstrate that the CUA Prototype, when installed and deployed, meets or exceeds the Prototype Solution's CUA evaluation results. The POP Test will be based on the functional requirements described in Appendix A – Capability and Usability Assessment (CUA) to the Statement of Work - Annex A of the Contract.

   ii) At the request of Canada, the Contractor must provide support and assistance with installation and deployment of its Prototype Solution in the RCMP Protected B Cloud Tenant.

   iii) It is Canada's intention that the POP Test be conducted at an RCMP location in the National Capital Region provided by Canada that recreates the technical environment described in Section 4.5 - Target Architecture. However, Canada reserves the right to conduct the POP Test at another location in Canada selected by the top-ranked Contractor, if the Contractor assumes all responsibility for recreating the technical environment described in Section 4.5 - Target Architecture. It is within the Contracting Authority's sole discretion to determine whether the Contractor has accurately recreated this environment for the test.

b) If the Solution is delivered using SaaS products, the POP Test will be used to confirm that the CUA Prototype, when accessed via an RCMP web browser or thin client meets or exceeds the Prototype Solution's CUA evaluation results. The POP Test will be based on the functional requirements described in Appendix A – Capability and Usability Assessment (CUA) to the Statement of Work - Annex A of the Contract.

c) The Prototype Solution deployed for POP purposes must be a production quality working Prototype Solution. The CUA Prototype will be used as a Minimum Viable Product (MVP). Features and functionality described in Appendix C – NCS Business Capability Model will be added to the MVP during Phase 2 of the project. The Prototype Solution deployed for POP test purposes must not require extensive redevelopment prior to successful deployment.

2.6 Phase 1 Deliverables

a) The Contractor must execute the NCS Phase 1 deliverables as described below.

   i) **Prototype Phase Kick-off Meeting** which must be scheduled no later than two (2) weeks from Contract award and which must:

(1) Occur virtually via video conference, teleconference or at a mutually agreed location in Canada's National Capital Region (in accordance with federal government guidelines related to COVID-19);

(2) Be chaired by the Public Services and Procurement Canada (PSPC) Contracting Authority;

(3) Include an agenda of the meeting and a presentation, if applicable, to be provided to the PSPC Contracting Authority at least 2 business days prior to the kick-off meeting; and

(4) Following the kick-off meeting, the Contractor must prepare and submit the minutes of the meeting to the Contracting Authority for approval within 2 business days, prior to distribution to all Authorities.

ii) **Mandatory Contractor Engagements Sessions**, which represent:

(1) A collaborative opportunity for the RCMP Business Client and Technical Authority to interact with the Contractor throughout Prototype development to answer questions on the NC3 mandate and requirements, and provide feedback on the prototypes, thus ensuring a thorough understanding of the requirements while promoting users at the forefront. A minimum of 3 sessions with each Contractor are planned. At Canada's sole discretion, additional sessions may be added if required.

iii) **Prototype Solution Installation Plan**, (if applicable per the Contractor's Cloud Service Delivery Model), for the Prototype on Platform (POP) Test, which must include but not be limited to:

(1) A set of instructions (i.e., installation manual) that is clear and sufficiently detailed to provide Canada with a full understanding of the installation requirements of the Prototype Solution.

(2) A technical description of the packaging or distribution method or installation archive for each of the infrastructure components and software components used in the Prototype Solution.

Note: Prototype Solution installation will be conducted by the RCMP IM/IT Program drawing on the Contractor for technical support and assistance on an as needed basis.

iv) **Prototype Solution Acceptance Test Plan**, for the POP Test (if applicable), which must include:

(1) A description of the procedures for planning, preparation, and completion of the POP acceptance tests.

Note: POP Test Acceptance evaluation criteria will be based on the CUA Evaluation results of the Contractor's Solution and will be provided by the RCMP.

v) **Prototype Solution and Documentation**, which must include:

(1) Access for 100 Users, with all Solution usage rights, grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada; and

(2) Support documentation or help files for each CUA Scenario (User Story).

vi) **Project Management Plan for Phase 2 Work – High Level Draft,** as described in Section 6.5 and Section 7.2, a), iii – Project Management Plan of this SOW for details.

vii) **Solution Implementation Plan for Phase 2 Work – High Level Draft,** as described in section 7.2, a), vi – Solution Implementation Plan of this SOW for details.

Table 2-1: Phase 1 Deliverables

No.	Description of Deliverable	Delivery Dates
1	**Prototype Phase Kick-off Meeting**	2 weeks from Contract award date
2	**No 1 – Contractor Engagement Session**	5 Weeks from Contract award date
3	**No 2 – Contractor Engagement Session**	10 Weeks from Contract award date
4	**No 3 – Contractor Engagement Session**	15 Weeks from Contract award date
5	**Prototype Solution Installation Plan**, digital copy delivered to Client Technical Authority and Contracting Authority	16 Weeks from Contract award date
6	**Prototype Solution Acceptance Test Plan**, digital copy delivered to Client Technical Authority and Contracting Authority	18 Weeks from Contract award date
7	**Prototype Solution and Documentation** (including access for up to 100 Concurrent Users), digital copy delivered to Client Technical Authority and Contracting Authority	20 Weeks from Contract award date
8	**Project Management Plan for Phase 2 Work – High Level Draft**, digital copy delivered to Client Technical Authority and Contracting Authority	21 Weeks from Contract award date
9	**Solution Implementation Plan for Phase 2 – High Level Draft**, digital copy delivered to Client Technical Authority and Contracting Authority	21 Weeks from Contract award date

3. Phase 2 – Full Solution

a) All work, listed under article 3 to article 7 of Phase 2 – Full Solution is subject to and contingent upon, at Canada's sole discretion, Canada's decision, to exercise the irrevocable option under article 7.1 c) i) in the Contract to authorize the Contractor to perform all or a portion of the Work described.

3.1 Scope of Work

a) The Contractor must deliver a Full Solution containing all functional and non-functional capabilities as described in Appendix C – NCS Business Capability Model.

b) The Solution must provide scalability and elasticity (up and down) to accommodate for fluctuations in business operational volumes.

c) The Solution must use an extensible architecture in order to take advantage of possible future technology, architectures and industry trends in the cyber security field.

d) The Solution can be delivered internal to the RCMP (IaaS or Private PaaS on an RCMP Protected B cloud tenant) with the grant of perpetual licenses; as a Software as a Service (SaaS) or Public PaaS; or a combination of SaaS and Perpetual Licenses herein referred to as a "Hybrid".

e) The Solution may be comprised of any combination of commercial-off-the-shelf (COTS), custom software and may include open source software and integrated software using APIs, however the resulting configuration must comply with the requirements described in this SOW.

f) The Solution must support the estimated numbers of Solution Core Users with access/rights to use the Solution, and Police and Partner Portal Users with access, upload and information consumption rights as provided in Appendix F – Volumetrics.

g) All proposed SaaS, Public PaaS and Private PaaS proposed in the Solution (including SaaS or PaaS components used in the case of a Hybrid) must be qualified per the Government of Canada SaaS-RFSA at Tier 2 Assurance level (Protected B) or the SSC GC Cloud Brokering Service Protected-B Public Cloud Services Catalogue.

h) The Contractor must install and deploy the Solution per their Solution Cloud Service Delivery Model (CSDM) (CSDM to be provided with System Architecture Documentation) and be compatible to the existing GOC Network Infrastructure and security configuration in place.

i) The Contractor must provide professional services and training services, on an as-and-when-requested basis in accordance with section 6.6- Project Resources and section 3.10-Training of the Statement of Work.

3.2 Use of Artificial Intelligence

a) The Solution must make use of Artificial Intelligence (AI) methods and techniques that comply with the Government of Canada's Directive on Automated Decision-Making[1], to enhance the Solution and benefit the NC3 business functions such as:

i) Machine Learning (ML);

[1] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

ii) Natural Language Processing (NLP);

iii) Pattern Recognition;

iv) Named Entity Recognition;

v) Topic Recognition;

vi) Sentiment Analysis;

vii) Decision-Making;

viii) Big Data Processing;

ix) Real-Time Analytics;

x) Text Analytics;

xi) Intelligence Analysis; and

xii) Trend Analysis.

b) The Contractor's Solution must provide Canada with an acceptable degree of transparency in the AI methods and techniques deployed. At the request of Canada, the Contractor must describe in detail AI findings for Canada's records and for potential use in judicial proceedings. Automated decision-making processes must be capable of being monitored to provide transparency and ensure against bias. The application of AI methods and techniques in the Solution must support the RCMP's obligation to comply with the Government of Canada's (GC) Directive on, Automated Decision Making[2] and guidelines on Responsible Use of Artificial Intelligence[3].

3.3 Information Management Requirements

a) The Solution must support and meet Canada's Information Management (IM) requirements by providing, at a minimum, the following IM functionalities:

i) Perform full text search on the metadata and data held within the Solution;

ii) Restrict access rights and un-restrict access rights to information and data subject to legislative requirements. Access will be required by an information management access role;

iii) Provide an audit trail of all events to demonstrate data integrity (e.g., creations, modifications, deletion, archiving, alienation (transfer outside the control of the government), down time, system failures and access associated to the information and data);

iv) Retain information and data held in the Solution for a specified period of time based on NC3 information retention requirements (e.g. Minimum of 10 Calendar years);

v) Purge information and data from the Solution at the end of their associated IM retention period, including information stored in an archived location within the Solution;

vi) Override disposition dates (purge dates) in the event of a legal or business requirement within the Solution;

---

[2] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

[3] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html#toc1

vii) Export information and data from the Solution in a compatible format as identified by business line and IM;

viii) Identify information and data that is disclosed for legislative requirement; and

ix) Add metadata fields to describe data in accordance with Government of Canada's, Standard on Metadata[4].

3.4 Software Solution and Documentation

a) The Contractor must provide a full roll-out of a configured, tested and implemented Solution and documentation for an estimated average of 500 concurrent Users at all levels nationwide and across federal law enforcement agencies, including Solution access for an estimated 2000 Users, which includes all Solution usage rights, grants, Software Documentation, Warranty, Maintenance and Support (excluding Training), waivers, non-disclosure agreements or other releases to Canada.

b) This deliverable includes all of the software and documentation related to all aspects of the Contractor's Solution including Operating System, system administration documentation, user guide documentation, custom developed source code and system maintenance documentation not specifically identified as a deliverable; however, it forms part of the documentation for the overall Solution.

c) The documentation must be prepared using Canada-approved Microsoft Office applications (Word, Excel, PowerPoint, Visio, Project, and Access) and must be legible and suitable for reproduction. Pages must be sequentially numbered. All attachments must be identified and referenced in the text of the document. If the Contractor's proposed Solution is based on a COTS product, existing documents must be modified to satisfy this deliverable.

d) It is the Contractor's responsibility to include the software and documentation that are required to describe with enough detail the functional, technical, and support aspects of the Solution.

3.5 Solution Technical Documentation

a) The Contractor must provide a System Design Document (SDD) that addresses the design of the delivered Solution. The Contractor's SDD must provide a single integrated view of the overall architecture for the Contractor's delivered Solution. The SDD must include the proposed Solution Cloud Service Delivery Model. This SDD must reflect the final architecture and configuration, including security configuration, of the Solution.

b) The following documentation must be provided to Canada as part of the Solution. They may be delivered as individual documents or packaged into other deliverables:

i) System architecture including a complete Solution architecture, Cloud Service Delivery Model and network and data flow diagrams (See Section 4 - System Architecture for details);

[4] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18909

ii) Security Assessment & Authorization (SA&A) that must include, at a minimum, a Statement of Sensitivity (SOS), Security Categorization, Security Concept of Operations and a Plan of Action and Milestones. The full list of deliverables for the SA&A will be provided by the RCMP Departmental Security Branch (DSB) once the prototype phase has passed and a view of the Solution is available.

iii) Security Management Plan that describes:

(1) Security controls to be implemented and monitored based on the Contractor's security assessment;

(2) The Contractor's roles and responsibilities for security (for complete details see Section 5 - System Security Plan);

(3) The physical location of any personnel engaged in security, configuration or support;

(4) Process to identify, report and respond to security incidents; and

(5) Security hardening of systems including ongoing patch management;

iv) Backup and Recovery Plan;

v) Information Technology Continuity Plan (ITCP) to ensure that the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are met;

vi) User and Administrator Training Plan;

vii) Configuration Management Plan;

viii) System Security Plan including auditing and logging (Section 4.9 - Logging and Auditing);

ix) User training material; and

x) Information Life Cycle Plan; from original creation of data through to final disposition and disposal.

c) The Contractor must ensure that the Solution technical documentation is accurate and kept up to date to reflect the Solution.

3.6 Disaster Recovery Plan

a) The Contractor must deliver to the Technical Authority a Disaster Recovery Plan (DRP) for the Solution. This must include a set of policies, tools and procedures to enable the recovery and continuation of the Solution operation following a natural or human-induced disaster.

b) The Contractor must work collaboratively with Canada to ensure that the DRP for the Solution integrates effectively with the RCMP's more broadly-based DRP for the enterprise technology infrastructure and critical application systems operating within.

c) The Contractor must provide Canada with a DR Testing Plan that documents:

i) Yearly testing procedures to confirm that DR is implemented correctly and satisfies applicable standards as specified in 3.15 Solution Availability and Performance.

ii) The expected and actual results of DR Testing; and

iii) For each deviation from the expected result, a description of the corrective measure(s) and timeline to implement.

d) The DRP must describe in sufficient detail how Canada can quickly recover and resume work after a major unplanned incident affects the Solution delivered by the Contractor.

e) The Contractor must describe the approach to achieving Solution recovery and the approach to data recovery. The data recovery approach must refer to the plan documented in Section 3.5- Solution Technical Documentation, the Backup and Recovery Plan and Information Technology Continuity Plan.

3.7 Solution Acceptance Test Plan

a) The Contractor must prepare a Solution Acceptance Testing and Quality Management Plan that describes how the functional and technical capabilities and processes will be tested in order to provide assurance to Canada that the Contractor's testing and quality management plans are in alignment with the NCS Business Capabilities Model and other requirements as defined in this SOW.

b) The Solution Acceptance Testing and Quality Management Plan must be approved by Canada. Acceptance Testing of the Solution must be conducted in accordance with the approved Acceptance Testing and Quality Management Plan and in alignment with the approved Solution Implementation Plan.

c) During development of the Solution, the Contractor must participate in quality management activities including reviews with Canada resources and Solution Users as well as testing (performance and regression) of various components and features of the system as needed to ensure acceptance.

d) The Contractor's methodology must follow principles and values allowing for frequent quality and review steps to be built in throughout the delivery and integration process. It is expected that features of the Solution will be developed and deployed through multiple iterations or sprints to enable incremental delivery of functionalities over the duration of the Contract.

e) The Contractor's methodology must include Testing Plans that include:

i) User Acceptance Testing;

ii) Regression Testing;

iii) Pre-installation Testing;

iv) Security Testing;

v) Volume Testing, including Large Data Set Analysis;

vi) Performance Testing (in consideration of Performance Metrics provided in Section 3.18 Performance Metrics); and

vii) Smoke Tests.

f) The Solution Acceptance Testing and Quality Management Plan must describe the Contractor approach to the following best practices:

i) Test data for:

(1) Unit Testing (including data and field validation testing);

(2) Sprint Testing;

(3) Integration Testing;

(4) Stress Testing;

(5) Regression Testing; and

(6) User Acceptance Testing.

ii) Testing and acceptance includes:

(1) Sprint Testing;

(2) Collaboration with stakeholders;

(3) Definition of “Done”; and

(4) End-to-end unit, functional, usability, accessibility, error, exception, compliance, interoperability, integration, and security (including vulnerability assessment scans) testing; and

(5) Disaster Recovery Testing.

iii) Maintenance Release and Patch Testing including regression testing due to updates to the Solution;

iv) A description of how automated testing is incorporated into Solution testing;

v) Test each sprint and include the test results in each requirement’s definition of Done;

vi) Address quality both reactively through testing and proactively encouraging practices to set the stage for quality work. Examples of proactive quality approaches include face-to-face communication, pair programming, and established coding standards; and

vii) Create and test riskier features in early sprints when sunk costs are still low.

g) The format of this deliverable is flexible and left to the Contractor to decide the best format and number of artifacts (e.g., diagram, views, models, catalogs, matrices) that are needed. Artifacts submitted must be clear and concise, well-described, and allow Canada to understand how the requirements are being met.

3.8 Solution Acceptance Test Report

a) The purpose of this report is to document the Acceptance Test results performed on the Solution prior to final acceptance by Canada.

b) The Acceptance Test Report must record the results of acceptance tests performed on the Solution. This report must either specify to Canada that the Solution has passed the required acceptance tests and meets the functional and technical requirements as stated in the Contract; or has failed the acceptance tests with reasons for failure and a corrective action plan by the Contractor.

3.9 Incremental Solution Deployment

a) The Contractor must, using an iterative approach, in collaboration with the RCMP, continuously develop features listed in the Product Backlog that will be prioritized in collaboration with the RCMP Business Client.

b) The Contractor must deliver, for acceptance, incremental releases of the Solution until Full Operating Capability is delivered as documented in the Business Capability Model.

3.10 Training

3.10.1 Training Plan

a) The Contractor must provide a Training Plan that describes how and when training will be delivered for Power-Users, SMEs, end users and technical support personnel.

b) The Contractor's Training Plan must describe Power-User and SME training using a "Train-the-Trainer" framework. The RCMP requires Solution usage and instructional training (how to teach the Solution) to potential instructors, Power-Users and SMEs to enable them to train their colleagues on how to use the Solution.

c) The Contractor's Training Plan must describe applicable Technical Resource training for Technical Support personnel.

d) The Contractor's Training Plan must describe how training would be delivered to small-groups of users (Power-Users, SMEs, End-Users or Technical Resources) on an as needed basis.

e) The Contractor's Training Plan must describe how Initial and updated bilingual (English and French) training resources will be provided including:

   i) Online Help;

   ii) Online Training;

   iii) English and French Documentation;

   iv) Updated training materials over time to cover newly-added functionality; and

   v) A description of the training materials to be provided.

3.10.2 Training Material

a) The Contractor must provide English and French electronic copies of operating manuals, technical manuals, and other relevant user documentation that is required in order to learn, use, and maintain the Solution.

b) The operating manuals, technical manuals, and other user documentation provided by the Contractor to Canada for use with the Solution must describe the operation of the Solution in sufficient detail to enable employees of Canada to use all of the functions and features of the Solution without assistance from the Contractor.

c) The Contractor must deliver bilingual (English and French) operating manuals and training materials using Canada approved Microsoft Office applications (Word, Excel, PowerPoint, Visio, Project, and Access).

d) Data and documentation used for training purposes must not contain any Protected information. Cybercrime data in the training environment must be fictional with no semblance to non-fictional person or data.

3.10.3 Training Delivery

a) The Contractor must provide Solution training to forty (40) NCS Power-Users and SMEs using a "Train-the-Trainer" framework.

b) The Contractor must provide applicable Solution technical training to twenty-five (25) technical support resources who are responsible for the on-going maintenance and support of the Solution.

c) The Contractor may be requested to deliver Solution training to small-groups of users (Power-Users, SMEs or Technical Resources) on an as needed basis.

d) Any requirements for training beyond the delivery of initial Power-User, SME and Technical Resource training will be completed through individual Task Authorizations.

3.11 Privacy Impact Assessment

a) The Contractor must work collaboratively with Canada to deliver a Privacy Impact Assessment (PIA) document that will, at a minimum, include the following information:

i) A list of all measures being taken by the Contractor to secure the Personal Information and the Records in accordance with the statutory obligations;

ii) Business processes, data flows and procedures for the collection, transmission, processing, storage, disposal, and access to information including Personal Information; and

iii) Any privacy-specific security requirements and Contractor recommendations that need to be addressed by Canada.

b) The Contractor must specifically address the following PIA items in detail:

i) The Solution's privacy protection strategies including detail on how Personal Information will be treated over its lifecycle;

ii) How Personal Information will be collected, used, retained, disclosed, and disposed only for the purposes of the Work specified in the Solution;

iii) How the Personal Information and Records will be accessible only to authorized individuals (i.e., on a need to know basis) for the purposes of the Work specified in the Solution;

iv) A preferred privacy breach protocol;

v) How the Contractor intends to ensure that Canadian Privacy requirements, as outlined in the Privacy Act[5], the Access to Information Act[6], and the Library and Archives of Canada Act[7], will be met throughout their performance of work for the duration of the Contract;

vi) Any new measures that the Contractor intends to implement in order to safeguard the Personal Information and the Records in accordance with their security classification;

vii) How the Contractor intends to ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification; and

viii) Describe how the Contractor intends to ensure that their staff is trained on privacy and privacy related principles.

---

[5] https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html

[6] https://laws-lois.justice.gc.ca/eng/acts/a-1/

[7] https://laws-lois.justice.gc.ca/eng/acts/L-7.7/index.html

c) The Contractor must provide a detailed explanation of any potential and actual threats to Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks.

d) The Contractor must demonstrate that the GC's sensitive and proprietary data and information will be properly protected and secured.

e) The Contractor must demonstrate how they will efficiently balance the need for high-quality testing and the protection of user information.

3.12 Transition Plan

a) The Contractor must deliver a Transition Plan that describes how the Solution will be brought to full operational status and integrated into the RCMP's target architecture (refer to Section 4.5 - Target Architecture) and Business Program Operations.

b) The transition plan must contain a brief description of the major tasks involved in the handover process, the resources needed to support the operations of the Solution, and any site-specific ongoing maintenance requirements.

c) During the transition period, the Contractor must undertake activities to ensure that efficient, and complete transition of the Solution occurs without interruption of service delivery to Canada.

d) The Project Transition Plan must include at a minimum:

   i) Activities and documents required to complete final handover and knowledge transfer from the Contractor to Canada's resources for life cycle operations and maintenance;

   ii) Key milestones that mark significant checkpoints along the transition timeline that can measure progress and outcomes;

   iii) Transition schedule;

   iv) Responsibilities and assignments that define who is responsible for—and assigned to—carrying out the activities;

   v) Planning Assumptions that are made in the development of the transition plan; and

   vi) Transition risks, including category of risk and mitigation measures.

e) The Contractor must undertake all obligations contained within the Transition Plan in accordance with the Transition schedule.

f) During the Transition period, the Contractor must provide transfer of knowledge to Canada as outlined in the Transition Plan.

g) The Contractor must respond to queries regarding Transition activities and any in-progress work to ensure a smooth transition and uninterrupted service delivery to Canada.

h) The Contractor will deliver the Transition Plan and updates in accordance with the schedule described in the list of Phase 2 deliverables herein.

3.13 Transition Out Plan

a) The Contractor must deliver a Transition Out plan (applicable to SaaS and Public PaaS) that describes the activities and processes required in the event that a SaaS or Public PaaS product agreement is terminated (e.g. SaaS or PaaS provider goes out of business).

b) The Transition Out Plan must include provisions for:

   i) Returning data and records to Canada, in both the vendors format and a platform-agnostic format;

   ii) Secure and permanent disposal of information assets and resources (e.g. equipment, data storage, files, and memory) from the vendor environment;

   iii) Secure and permanent disposal of Information Assets that are created by replication to support high availability, back-ups and disaster recovery;

   iv) Assistance from the Contractor in carrying out all activities related to Transitioning out of a SaaS or Public PaaS; and

   v) Business continuity.

c) The Contractor must, upon request by Canada, provide evidence that demonstrates successful and permanent erasing, purging or destruction of all resources related to Canada's use of the SaaS or Public PaaS.

d) The contractor must, in the period leading up to the end of the Contract Period, if Migration or Transition Services are requested by Canada, assist Canada in the transition from the Contract to a new contract with another supplier and or migrate the RCMP's Data to a new supplier environment.

3.14 Solution Maintenance and Support

3.14.1 Software Warranty Period

a) In this SOW, unless provided otherwise in the Contract, Software Warranty Period means a period of twelve (12) months from the date on which the Licensed Software is accepted in accordance with the conditions of the Contract, except for warranty work and any other work that is scheduled under the Contract to be performed after the start of the Software Warranty Period.

3.14.2 Evolution of Solution

a) In an environment where technology is rapidly changing, and cybercrime practices are evolving, the Contractor must demonstrate ongoing plans and product roadmaps as well as provide advice and insight to trends to ensure the Solution remains aligned with industry best practices, technology and analytics advancements throughout the contract period, and until the completion of the warranty period.

b) The Contractor's Solution must allow for presentation layer customization, enabling the RCMP to build out new workflows, approval processes, role definitions, access rights, templates, reports and screens, in order to provide additional functionality not provided in the original solution.

c) The Contractor must provide a means of collaborating with the RCMP on the development of new functionality updates as well as maintenance patches; both during development and after the delivery of Full Operating Capability.

3.14.3 Support and Maintenance

a) Until the completion of the warranty period, the Contractor must:

i) Track incidents and cases through the RCMP's ticket management system. Weekly and monthly reports on incidents (tickets) and their resolution are required and must be delivered to the Technical Authority; some incidents may require Contractor presence on site in Canada's National Capital Region.

ii) Hold monthly meetings to discuss major incidents with the Solution and share knowledge of ongoing development solutions and initiatives. The ticket should describe the issue and incidents in detail, ensure that reviews were performed, corrective measures were approved, and that post-incident Quality Assurance (QA) activities were completed.

iii) Ensure that the Contractor's personnel are qualified and able to respond to client and User questions and, to the extent possible, be able to resolve User problems by telephone or email and provide advice regarding functionality, configuration, and technical issues.

iv) Must notify Canada of forthcoming changes and potential operational issues with new releases for the Solution and provide notifications to Users of any changes that may impact service.

v) Must provide a documented, incident-prioritization procedure that includes definitions for the severity of issues (e.g., critical, major, and minor) and their associated response and resolution times.

vi) Must assign an account representative as an escalation point for support and account issues.

vii) Provide Level 3 Support of the complete Solution along with development, implementation, configuration and support of new features. The expectation is that Canada will have support responsibilities for the service (i.e., first-level support and managing the renewal of all software and tenant licencing). See Annex D - Definitions and Interpretations for definitions of the Support Levels.

viii) Include Support capabilities, including training of features and enhancements.

3.14.4 Event and Incident Management

a) The Contractor must cooperatively work with Canada and any other third parties as requested by Canada in order to resolve incidents, as follows:

i) The Contractor must provide Canada with status updates of Incidents with priority levels specified by Canada and at a frequency specified by Canada. The status updates must be provided by email and when requested by Canada, provided verbally;

ii) The Contractor must provide an estimated time for resolution with each update within the Incident Ticket and when requested by Canada, provided verbally;

iii) The Contractor must ensure progress and updates, root cause, and resolution have clear descriptions using complete words, sentences, and proper grammar in English or French;

iv) When creating or updating an Incident Ticket the Contractor must use the RCMP's ticket management system;

v) The Contractor must document in the Incident Ticket Activity Log, all:

(1) Management and technical escalations for Incidents;

(2) Interactions with third parties; and

(3) Investigation, troubleshooting details, analysis details, resolution activities, and communications for Incidents in the Incident Ticket Activity Log.

vi) The Contractor must record in its Incident Ticket, any direction that Canada provides that are related to the frequency of updates, change in priority, and escalation including the name of the RCMP representative providing each direction;

vii) The Contractor must identify and document the causal factors (i.e., root causes) of all Incidents when known; and

viii) The contractor must develop workarounds to address incidents wherever possible, until the root cause of the incident has been addressed (or where root causes are unknown).

ix) The Contractor must provide a briefing for an Incident within one (1) working day of a request by Canada for an Incident. The briefing must be based on a format specified by Canada.

x) The Contractor must work with Canada to develop and implement post incident reports and preventative action plans. The Contractor must notify Canada in advance when the Contractor becomes aware that it will not meet target dates specified in its action plans.

xi) The Contractor must provide Canada with a clear description of each tool, system, and application that is used by the Contractor or made available to Canada.

3.15 Solution Availability and Performance

a) The Solution must be available for use twenty-four (24) hours a day and three hundred and sixty-five (365) days a year with 99.45% uptime averaged over a month.

b) For the purpose of Business Continuity Planning for NCS;

i) Maximum Allowable Downtime for NCS is 4 hours;

ii) Recovery Time Objective is 1 day; and

iii) Recovery Point Objective is 4 days.

c) For the purpose of Business Continuity Planning, the minimum service levels Canada will be seeking to support during a recovery period are, in reference to Appendix C – NCS Business Capability Model:

i) 3.0 NCS – Police and Partner Portal (P3) Capabilities, and

ii) 4.0 NCS – Functional Services Capabilities, supported by a subset of,

iii) 5.0 NCS BCM - Solution and Technical Capabilities.

Capabilities defined in 1.0 Public Reporting are the responsibility of the RCMP and capabilities defined in 2.0 NCS – Case Management Capabilities are subject to a lower priority restoration of service level objective.

d) The Solution must be able to support, at minimum, the volumes detailed in Appendix F - Volumetrics herein without a degradation in performance.

e) Canada has the responsibility for supporting the availability and performance of the Public Reporting Website.

3.16 Users

a) The Solution must be capable of supporting up to five hundred (500) concurrent users while processing the volumes described in Appendix F - Volumetrics before degradation of performance.

b) See Appendix F - Volumetrics for estimates of total Core Users (Internal to NC3 and RCMP) that will have access/rights to use the solution and Police and Partner Portal Users who will upload and consume the information collected by the Solution via the Police and Partner Portal.

3.17 Solution Volumes

a) See Appendix F - Volumetrics for volume growth estimates of Solution usage over Eight (8) years.

b) The data is provided for informational purposes and does not represent a commitment that Canada's future usage will be consistent with this data.

c) The Contractor's Solution must provide elasticity and scalability to account for lower or higher than estimated user, transaction growth and data volumes as well as short term fluctuations in data acquisition and processing patterns.

3.18 Performance Metrics

Based on estimated Solution volumes and user support requirements, the Solution must meet the following performance requirements;

Table 3-1: NCS Maximum Response Times

Component	Representative Activities	Max. Response Time (Seconds)
NCS User Interface	• Login • Open a Data View/Entry/Edit Screen • Save a Transaction • Forward or Assign a Task/Work Item	1
	• Query NCS Data Repository (Display Query Results)	Avg. 2 sec – max. 5 sec

Component	Representative Activities	Max. Response Time (Seconds)
	• Open a Queue • Open a dashboard screen	2
Police and Partner Portal User Interface	• Login • Open a Data Entry Page • Save Transaction	1
	• Query NCS Data Repository (Display Query Results)	Avg. 2 sec – max. 5 sec
	• Open Dashboard • Open a Queue	Avg. 2 sec - max. 3
Indexing / Parsing	• Automated Data Extraction • Data Ingestion of Structured and Unstructured Data (email, P3 Request)	Near Real Time
Correlation	• Match Extracted data to NCS Repository • Match new submissions against existing data	Near Real Time

3.19 Official Languages Act[8]

a) The Solution must comply with the Official Languages Act including at a minimum the following:

i) The quality and level of language in the Solution and associated messages, instructions, software, and documentation must be equivalent in English and French.

ii) Error messages from the Solution must appear in the User's language of preference or be bilingual and must be equivalent in English and French.

iii) The instructions and directives stemming from the Solution must appear in the User's language of preference.

iv) Titles in full in the Solution must have the same meaning in both official languages.

v) Alternate texts for accessibility must be produced in the language chosen by the User of the Solution.

vi) Legends and texts of the Solution images and graphics must be produced in the same way in both English and French.

vii) Reports must be produced in the language requested by the User or be bilingual (English and French).

viii) When a User changes their language of preference within the Solution, the change must apply immediately, without the User having to exit the interface.

[8] https://laws-lois.justice.gc.ca/eng/acts/o-3.01/

ix) Use universal icons (standards) for various menus and tools of the Solution (if possible), instead of EN or FR elements in full, with mouse-over display and alternate text in the language chosen by the User.

x) A search carried out in the graphical interface of the Solution must yield the same results in both English and French. If the same search criteria is entered in both a French UI and an English UI – the result should be the same.

xi) Help documentation must be provided in both French and English.

xii) The instructions and directives for the Help page must be provided in both Canadian official languages.

xiii) Contractor Support Call Centres must provide equivalent services in both Canadian official languages.

3.20 Web Content Accessibility Guidelines (WCAG)

a) The Solution must comply with the WCAG 2.0[9] and Government of Canada's Standard on Web Accessibility[10] as follows:

i) The Solution must be accessible using assistive technologies and various Web browsers, such as Internet Explorer, Firefox, Chrome, Safari and Edge.

ii) Information, structure, and relationships conveyed through presentation must be programmatically determined or are available in text.

iii) When the sequence in which content is presented affects its meaning, a correct reading sequence must be programmatically determined.

iv) All functionality of the content must be operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the User's movement and not just the endpoints.

v) If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface, and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the User is advised of the method for moving focus away.

vi) A mechanism must be available to bypass blocks of content that are repeated on multiple Web pages.

vii) When any user interface component receives focus, it must not initiate a change of context.

viii) Changing the setting of any user interface component must not automatically cause a change of context unless the User has been advised of the behavior before using the component.

ix) In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements must not contain duplicate attributes, and any IDs must be unique, except where the specifications allow these features.

---

[9] https://www.w3.org/TR/WCAG20/

[10] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

x) For all user interface components (including but not limited to: form elements, links and components generated by scripts), the name and role must be programmatically determined; states, properties, and values that can be set by the User must be programmatically set; and notification of changes to these items must be available to User agents, including assistive technologies.

xi) Content must not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential.

xii) Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages must occur in the same relative order each time they are repeated, unless a change is initiated by the User.

xiii) Components that have the same functionality within a set of Web pages must be identified consistently.

xiv) Any keyboard operable user interface must have a mode of operation where the keyboard focus indicator is visible.

4. System Architecture

a) The Contractor must deliver an Architecture describing the fundamental organization of the Solution to Canada. The Architecture must include the Solution Cloud Service Delivery Model, components that comprise the Solution, the relationships between components, and the environment, connectivity to the network in the architecture as well as data flows, and the principles guiding the design, development, and deployment of the Solution.

b) The format for delivering the Architecture is flexible and left to the Contractor to decide the best format and number of artifacts (e.g., diagram, views, models, catalogs, matrices) that are required. Artifacts submitted must be clear and concise, well-described, and allow Canada to not only understand the Solution but how the requirements are being met.

4.1 General Requirements

a) The following points provide high-level guidance to the Contractor and must not be considered as an exhaustive list of requirements or deliverables:

i. The Contractor must describe how the proposed Architecture will adhere to the Target Architecture (Section 4.5 – Target Architecture) and where the Contractor's Solution differs, the Contractor must describe how the proposed architecture replaces or extends the Target Architecture.

ii. The Contractor must describe the Technical Architecture which includes the enabling technology stack and any required third-party products or services to support the implementation, configuration, and operation of the proposed Solution;

iii. The Contractor must describe the Network Architecture which includes any assumed integration points to GC infrastructure and the RCMP Protected B Cloud Tenant;

iv. The Contractor must describe the Information Architecture which includes any information flow and dependencies for data migration, backup, and recovery; and

v. The Contractor must describe the Security Architecture which addresses all of the security issues identified herein in Section 4.8 – identity and Access Management Identity and Access Management.

vi. The Contractor must describe the proposed Solution Cloud Service Delivery Model including detailed descriptions of:

(1) all Cloud Services and Resources to be hosted on the RCMP Protected B Cloud Tenant (IaaS and Private PaaS components);

(2) all cloud resources that the RCMP will need to provision to support the services and resources mentioned above (e.g. Compute, Data Storage, Network, Message Queuing etc.);

a. Include specific resource attributes (region, vCPUs, memory, # of instances, on-demand vs reserved, etc.). Include applicable CSP Part Numbers, SKU etc. in order for the Technical Authority to accurately cost Cloud resources to be provisioned by the RCMP;

(3) all Cloud Services and Resources hosted by the Contractor's Cloud Service Provider (Public PaaS or SaaS) including related status per SaaS-RFSA and SSC GC Cloud Brokering Service Protected-B Public Cloud Services Catalogue qualifications; and

(4) integration of the proposed Cloud Services and Resources into the Solution Architecture.

vii. The Contractor's Cloud Service Delivery Model must consider the following:

(1) Three separate environments: (1) Development, (2) Test, and (3) Production – with the ability to auto-scale each as needed;

(2) Elasticity and Scalability capabilities to account for evolving environment specific needs, lower or higher than estimated operational growth rates as well as unanticipated spikes in operational volumes;

(3) Business continuity and high availability requirements. Refer to SOW; Section 3.15 – Solution Availability and Performance;

(4) Cost Optimization, Operational Efficiency and Monitoring;

(5) Ability to meet stated performance metrics. Refer to SOW Section 3.18 – Performance Metrics; and

(6) Ability to service the year-over-year growth of User and Solution volumes. Refer to Appendix F - Volumetrics;

viii. Using Table 1 of Appendix G – Cloud Service Delivery Model Tables, provide a clear reference to allow the Technical Authority to identify all of the cloud resources that the Contractor's Solution requires the RCMP to provision in order to operate and support the Contractor's Solution.

b) The proposed Solution architecture must specify how it will adhere to the GC Digital Standards[11].

c) The proposed Solution architecture must specify how it will adhere to the GC Enterprise Architecture / Standards[12].

d) The Contractor should leverage COTS products or open-source components to deliver functionality where possible, as opposed to proprietary custom-developed solutions.

e) The Contractor must deliver an Architecture Roadmap to describe the components and features which they will deliver and a timeline of when these components will be included in the architecture.

4.2 Integration with RCMP Environment

4.2.1 Mandatory RCMP Holdings

a) The Contractor's Solution must use the RCMP enterprise standard holdings to deliver the portions of the Solution listed in the Description column in **Table 4-1: Mandatory RCMP Components**. Licenses consumed for these components must not be included in the costing of the Solution to Canada.

[11] https://www.canada.ca/en/government/system/digital-government/government-canada-digital-standards.html

[12] https://wiki.gccollab.ca/Government_of_Canada_Architectural_Standards

Table 4-1: Mandatory RCMP Components

Component	Description
Azure Active Directory	RCMP enterprise standard for identity and access management.
Environmental Systems Research Institute (Esri)	RCMP enterprise standard for GIS and mapping analytics.

4.3 Interoperability

a) The Solution must be configured to support interoperability with existing applications:

i) The Solution must provide an architecture that is extensible;

ii) The Solution must provide the ability for all business data to be extracted to an external data warehouse via bulk interfaces;

iii) File-based data extraction must support a wide variety of file formats;

iv) The Solution must provide the ability to export and import data via an Extract, Transform, and Load (ETL) capability either out-of-box or using other commercial platforms (e.g., IBM DataStage or other open-source products);

v) The Solution must provide the ability to import and export reference and business data received in bulk (e.g., from Law Enforcement Agencies, Users, legacy CAFC data) into or out of the NCS Data Repository via both an API and a bulk interface;

vi) The Solution must provide integration with existing CAFC systems and associated data;

vii) The Solution must provide the ability to invoke external synchronous web service APIs via open industry standards when the authoritative source of that data or functionality resides in other systems;

viii) The Solution must provide the ability to support Transport Layer Security (TLS) 1.2 encryption for all interfaces at a minimum level of connectivity security;

ix) The Solution must provide the ability for interfaces to effectively handle situations where external systems experience failure or are unavailable;

x) The Solution must protect information through secure authentication methods using open standards (including but not limited to OpenID, OAuth, or SAML);

xi) All APIs must be exposed via open standard bindings and protocols (including but not limited to: Representational State Transfer (REST) using JavaScript Object Notation (JSON) or Extensible Markup Language (XML) depending on the needs of the interfacing system;

xii) All APIs must be able to expose data as non-proprietary business entity or object schemas. Specifically, APIs must be able to abstract raw back-end table and data structures;

xiii) APIs must adhere to the Government of Canada Standards on APIs[13]; and

xiv) The Solution must have the ability to support the ingestion of data from external sources and reporting across multiple information domains using REST with JSON and XML.

4.4 Public Reporting Web Site

a) Background

[13] https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html

i) The Public Reporting Web Site, developed by the RCMP, provides an easy-to-use web site for victimized individuals and small and medium-sized enterprises to report a wide spectrum of cybercrimes including pure cybercrime (e.g., malware, hacking), financially-motivated cybercrime (e.g., cyber fraud, identity theft, forgery, extortion) as well as traditional fraud and scams.

ii) The public reports will be ingested by the Solution which will subsequently provide the various analytics, coordination, and deconfliction components to add value through data enrichment. Using the P3, the Solution will have the ability to share the report with the appropriate Police of Jurisdiction (POJ) based on the geolocation of the victim. Reports received through the cybercrime reporting web application will be stored in the Solution Repository provided by the Contractor.

iii) Public reports will include, at minimum (where available), the following data entity types and interface requirements:

(1) Consent Info: Consent to collect and share information;

(2) Complaint Info: One complainant including tombstone and contact info on the complainant, and possible information for a person reporting on behalf of another;

(3) Incident Info: One or more incidents including incident number, description, dates, locations, occurrences, money lost, assets affected, contact methods, personal information types at risk, devices involved, and social media accounts involved;

(4) Suspect Info: Zero or more suspect descriptions, including suspect clues (e.g., email, phone, web site, application);

(5) Evidence Files: Zero or more evidence file attachments including descriptions and metadata attributes. File types supported include, but are not limited to: HTML, JPEG, PDF, TXT, XLSX, XML, and PNG; and

(6) Cross-referencing of Incident Number from Public Report with a Solution Ticket number.

iv) The Public Reporting Web Site will publish completed valid complaint files to a queuing service that will be accessible to the Solution.

v) Note that the Public Reporting Web Site component is expected to be deployed in a container within the RCMP Protected B Cloud Tenant.

b) Requirements

i) The Contractor must provide a means of ingesting data from the Public Reporting Web Site into the Solution, in near real time, using an available RCMP Protected B Cloud Tenant queuing service for the communication.

ii) The Contractor Solution must have the capability of subscribing to the queuing service to receive each Public Reporting Web Site complaint file, through a RESTful API in order to begin the automated triage processing.

4.5 Target Architecture

a) The Target Architecture is a component-based view that depicts the high-level information flow between components to illustrate the requirements of the NCS project architecture (see Appendix D – High Level Architecture Diagram). The intent of this diagram is to provide a conceptual view to aid the Contractor in understanding the end-state vision during development of the Contractor's Architecture. The Contractor must provide a component-based design to facilitate implementation and future support needs of Canada.

4.6 Cloud Deployment

a) The Contractor must deliver a complete Solution consisting of any combination of Cloud Service Delivery Models including;

   i. Internal to the RCMP (IaaS or Private PaaS on an RCMP Protected B Cloud Tenant) with Grant of Perpetual Licenses – Solution deployed, operated, and managed by the RCMP on the RCMP's Protected-B Cloud Tenant using the Solution's applicable Cloud Service Provider (CSP) infrastructure;

   ii. SaaS or Public PaaS – Solution will be hosted and managed by the Contractor, on the Contractor's chosen CSP, and used by the RCMP; or

   iii. Hybrid Cloud Service Delivery Model – A combination of the above cloud Service Delivery Models.

b) The Cloud Service Providers must be successfully on-boarded to Shared Services Canada (SSC) and TBS's SCED (Secure Cloud Enablement and Defence[14]) project.

c) The Solution must be free of any known Critical and High Impact bugs (where Critical is defined as a showstopper to perform work and High Impact is defined as affecting system use severely and requires correction in next release), up-to-date and compliant with the specification describe within this document.

d) To ensure the Solution will be compliant, the following guidelines must be considered as part of the Architecture:

   i) The deployment of the Solution must be fully automated using declarative templates for infrastructure as code in an industry-standard format.

   ii) Installations of packaged software must adhere to RCMP enterprise deployment technologies (automated processes, scriptable configurations) (e.g., COTS products installed onto a Windows operating system must use Microsoft Endpoint Configuration Manager).

   iii) The Contractor must only use services that are on the approved list of Protected-B Cloud services provided by the GC, or services for which the vendor has received written approval from Canada. For a full list of approved Protected-B Cloud services, please refer to the GC Cloud Brokering Services Catalogue[15] or the PSPC Request for Supply Arrangement (SaaS-RFSA)[16].

---

[14] https://wiki.gccollab.ca/GC_Cloud_Infocentre

[15] https://cloud-broker.canada.ca/s/pbmmcatalogpage?language=en_CA

[16] https://www.tpsgc-pwgsc.gc.ca/app-acq/cral-sarc/saas-eng.html

iv) The Solution must use Azure AD (Active Directory) functionality for Identity and Access Management for Internal RCMP and external partner Users of the Solution.

(1) Managed identity and service principal for the IaaS and SaaS where available.

e) The Solution must implement the following practices:

i) PKI key management for the management and storage of cryptographic keys, application secrets, certificates and access tokens; and

ii) Encryption, including storage service encryption, disk encryption, and database encryption with the option for Canada to bring its own keys (Bring Your Own Key feature such as Software as a Service); and

iii) Encryption using Pretty Good Privacy (PGP) and x.509 must be seamlessly integrated to support cryptographic privacy and authentication of data communication as well as signing, encrypting and decrypting of e-mails and files to increase the security of email communication with partners.

f) The Solution must satisfy business continuity planning, high availability, and redundancy requirements for an enterprise-scale implementation. These requirements include support for redundancy and failover by utilizing multiple qualifying data regions or availability zones within Canada.

g) The Solution must enable the generation of logs (e.g., activities, states, errors, events) and metrics (e.g., consumptions, scales, performances) of the individual components that make up the Solution. The outputs of the logs and metrics must be in an industry standard format and support streaming to specified service endpoints within the RCMP Protected B Cloud Tenant.

h) For IaaS compute instances, operating systems must be limited to Windows or Linux (i.e., Red Hat, SuSE, or Ubuntu) and support the automation of patches and updates on a regularly scheduled basis.

i) The Contractor must compile a detailed list of software and infrastructure licences that will be required to implement the Solution including associated annual costing for the duration of the Contract.

4.7 Source Code and Development

a) The Contractor must, for parts of the Solution that involve custom code development and custom configuration, deliver a Solution in accordance with the following guidelines:

i) The Contractor must provide an integration team to work collaboratively with the RCMP to do all development work either using RCMP workstations, from RCMP premises, or via secure remote connection (pending impact of COVID-19 restrictions that may be in effect) within a separate subscription on the RCMP Protected B Cloud Tenant;

ii) The Contractor must provide an integration team to work collaboratively with Canada personnel to deploy releases and patching through a support agreement with Canada;

iii) The Contractor must ensure all integration components are clearly described and are API based with minimal custom code. All source code comments must be written in English only;

iv) The Contractor must develop updates and new features on the RCMP Protected B Cloud Tenant in a development environment. The methodology used must adhere to the GC Digital Standards especially with respect to Collaboration, Continuous Integration and Continuous Delivery (CI/CD). The Contractor is to disseminate information concerning installation and support through collaboration sessions with Canada to maintain a high level of application understanding;

v) The Contractor must manage the source code repository and pipeline within a specified RCMP controlled repository. The RCMP will provide Development, Test/QC and Production environments;

vi) The Contractor must package software code and all its dependencies so that it can be executed repeatedly and consistently on the Solution's infrastructure. This needs to allow for applications to be developed as write once, run anywhere (WORA) in a container-deployment architecture. These containers must be version-controlled and include deployment scripts. Install scripts—including back-out scripts and recovery plans—are required for all releases;

vii) The Contractor must collaborate with the RCMP to develop an RCMP Cloud DevOps technology stack for the Solution, that is compatible with the RCMP Protected B Cloud Tenant;

viii) The Contractor must work in collaboration with the RCMP to incorporate security scripts into the build process in order to verify that every build complies with an agreed upon list of security controls.

ix) The Contractor must deliver and maintain a Solution with a full set of automated unit and integration tests such that application testing (excluding accessibility and UAT testing) is completely automated. The Contractor must also support testing of maintenance patches and software updates as well as regression testing to ensure that the patches do not negatively impact existing functionality; and

x) The Contractor must deliver documentation describing key support methods, implementation plans, and deployment processes during integration into the RCMP Protected B Cloud Tenant. The Contractor is also required to provide updates to documentation during the release process before released into Production status.

4.8 Identity and Access Management

a) Identity and access management for the Solution will principally be handled through use of Microsoft Azure Active Directory (Azure AD) as detailed in the following sections. The Solution must allow for the granting, editing, and revoking of System Administrator access to all NCS components by the RCMP Cloud operations team through the Azure AD service.

b) While the responsibility for managing the contents of the Azure AD will reside with the RCMP, the Contractor must configure the Solution's components to use Azure AD as their directory service.

c) The access management capabilities for the Solution must be delivered using the roles, groups, identities, and attributes contained in the Azure AD service. The Contractor can request changes to the Azure AD roles, groups, identities, or attributes for the purpose of meeting access management requirements. The Contractor must submit a request to Canada providing the detailed information about the item(s) to be added and the access management reasons for the change(s) in order for a request to be considered.

d) The Solution must be capable of storing and managing public and private key certificates (PGP and x.509) associated to partner users.

    i) For example, during onboarding, the Solution should support capture of the partner user's PGP public key (or offer to generate a key pair for them if they don't have one), store it along with user account details and associate it with the applicable organizational email.

    ii) For the case of an RCMP employee wanting to generate a PGP key pair, the Solution could provide a wrapper that would tie into a key escrow/recovery service and associate it with their RCMP identity through email.

e) The Solution must be capable of providing login (Authentication) functionality per RCMP approved identity management standards and technologies at a minimum Level of Assurance 2 and Level of Assurance 3 as per the User Authentication Guidance for Information Technology Systems (ITSP.30.031 v3)[17].

f) The RCMP will provide a means of integrating the RCMP PKI credentials with Azure AD Two-Factor Authentication (2FA). The Solution must ensure that all access control decisions use the level of assurance of the authentication session.

4.8.1 System Administrator Identity and Access Management

a) The Solution must use Azure AD for identity and access management for the System Administrator (RCMP and external partners) of the Solution.

b) The Solution must provide an access management capability for System Administrator accounts through Role Based Access Control using the roles defined in the RCMP Azure AD.

4.8.2 Administrative Account Identity and Access Management

a) The Solution must use Azure AD for identity and access management for administrative accounts (such as, but not limited to, managed identities or service principal accounts) where it is supported, with the exception of standalone accounts as detailed in this section.

b) The Solution must provide an access management capability for administrative accounts, except for standalone administrative accounts, through Role Based Access Control using the roles defined in the RCMP Azure AD schema.

c) The creation of any standalone administrative account required by the Solution (such as one needed to configure an application to use Azure AD) must meet all the following conditions:

[17] https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3

i) A request to use the standalone account containing the application(s) and resource(s) that the account is used to access, the scope of the privileges the account holds, the authentication method used for the account, and the reason the account is required must be provided to Canada for each individual account.

ii) The request for the use of the standalone account must be approved by Canada prior to inclusion in the Solution.

4.8.3 NCS Access Management Components

a) All components of the Solution must allow for granular role-based access control based on Azure AD groups and attributes.

b) The Solution must have granular access control that will allow Canada to authorize generic activities such as creating, reading, updating, deleting, as well as specific capabilities for the individual services (such as, but not limited to, submitting exchange requests, file transfer requests).

c) The Contractor must work with the Canada to provide the granularity of access control needed to grant the appropriate level of access to each component of each service for the internal user and partner groups that will access it.

4.9 Logging and Auditing

a) The RCMP Security Information and Event Management (SIEM) capability must have the ability to aggregate and correlate Event and Audit Logs from all log sources as they pertain to the management and delivery of the Solution. Canada reserves the right to determine, prioritize, and ultimately digest event messages, information messages, alerts, and alarms. The Contractor must work with Canada to configure and manage the amount and type of logging being generated by the Solution.

b) The Contractor's Solution must integrate with the RCMP Protected B Cloud Tenant's log collection capability.

c) The Contractor must work with Canada to integrate with the RCMP SIEM capability, including but not limited to providing information required by Canada and implementing configurations and changes on the Contractor's Solution. Formats include Common Event Format (CEF), syslog, and other common log formats specified by Canada.

d) Integration must be through data feeds provided to the RCMP SIEM through one or both of the following methods:

i) Log data is transmitted from the Contractor to the RCMP Protected B Cloud Tenant's log collection capability using a format compatible with the RCMP SIEM; and

ii) Log data can be retrieved from the Contractor systems that support remote retrieval using the RCMP Protected B Cloud Tenant's log collection capability.

e) The Contractor must provide a mechanism to capacity-manage data transfer rates to the RCMP Protected B Cloud Tenant's log collection capability in order to remain within Canada-approved volumes. This includes but is not limited to:

i) If event rates are approaching an RCMP-specified limit, the Contractor must work with Canada to identify the reason behind the increase and to take the appropriate actions to revert or address the change.

f) The Contractor must provide a mechanism to ensure that Audit Logs can be collected from various systems, amalgamated centrally, and sent to the RCMP Protected B Cloud Tenant's log collection capability to be analyzed regularly by an automated tool.

g) The Contractor must build the Solution's logging capability to centrally store collected security and non-security events and packet traces within the RCMP Protected B Cloud Tenant's log collection capability.

h) The Solution must log the following information for all System Administrator activities including but not limited to:

   i) System Administrator identifier;

   ii) Date and time stamp of the activity;

   iii) Details pertaining to the activity performed; and

   iv) Data modified by the activity.

i) The Solution must provide logging of the following System Administrator account events:

   i) Account creation;

   ii) Account modifications;

   iii) Account disabling;

   iv) Account termination;

   v) Successful authentication; and

   vi) Unsuccessful authentication.

j) The Solution must provide logging information:

   i) What type of audit event occurred;

   ii) When (i.e., date and time) the audit event occurred;

   iii) Where the audit event occurred;

   iv) The audit source of the event;

   v) The outcome (i.e., success or failure) of the audit event; and

   vi) The identity of any User and subject associated with the audit event.

k) The Solution must log the following events:

   i) Use of privileged System Administrator accounts;

   ii) Accepted System Administrator login and logout with date and time stamps;

   iii) Rejected login attempts with date and time stamps;

   iv) Accepted System Administrator or User login and logout with date and time stamps;

   v) Grant, modify, or revoke access rights including adding a new System Administrator, User, or group, changing System Administrator and User privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and System Administrator and User password changes;

vi) Configuration changes including installation of software patches and updates or other installed-software changes;

vii) Process start up, shut down, or restart;

viii) Process abort, failure, or abnormal end especially due to resource exhaustion or reaching a resource limit or threshold (such as for Central Processing Unit (CPU), memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS), or hardware fault; and

ix) Detection of suspicious or malicious activity such as from a Host Intrusion Detection System or Intrusion Prevention System (IDS/IPS), antivirus system, or antimalware system.

5. System Security Plan

a) The Contractor must review and respond to all security requirements in Appendix E – Security Requirements Traceability Matrix (SRTM) with a proposed mechanism to address the requirement. In the event of any conflict between requirements in the entire RFP and the SRTM, the SRTM will take precedence.

b) The Contractor must address any risks identified by Canada's compliance processes such as audits, Security Assessment and Authorization (SA&A) Activities, Threat and Risks Assessments (TRAs), and Privacy Impact Assessments (PIAs).

c) The Contractor must allow Canada or its designees, at no cost to Canada to access the Contractors development and test environments within the RCMP Protected B Cloud Tenant to inspect and audit the Contractor's compliance with the privacy, security and information management requirements under the Contract and to have full access to all Personal Information and Records.

d) The Solution must allow Canada to install passive network tap(s), to enable a full sustained network capture of all Internet Protocol (IP) Layer network traffic and interactions between components within the NCS with the ability to inspect within encrypted traffic.

e) The Contractor must co-operate with any security audits or inspections requested by Canada by providing the following evidence:

   i) Data-flow documentation, data protection description, data architecture and security descriptions as they pertain to work under the Contract;

   ii) The Contractor's own PIAs, risk assessments, and risk treatment plans as they pertain to work under the Contract; and

   iii) Interviews conducted by Canada of the Contractor's employees and third-party consultants during normal working hours or other times as mutually agreed.

5.1 General Compliance Requirements

a) The NCS must be protected and secure in accordance with Government of Canada security policies and legislation. The Contractor must maintain the Security of the NCS in accordance with the ongoing Security requirements that follow:

5.1.1 Government of Canada Policy Compliance

a) The Contractor must comply with the following Government of Canada security policies and legislation for handling of Protected B information including any updates, abandonments or changes during the period of the Contract:

   i) RCMP G1-009 - Transport and Transmittal of Protected and Classified Information[18].

5.1.2 Third Party Assurance and Certifications

a) The Contractor must maintain the following valid and up-to-date industry certifications for the period of the Contract:

[18] http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-eng.htm

i) ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems Requirements[19];

ii) ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls[20] based on ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls for cloud services;

iii) ISO/IEC 27018:2019 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors[21]; and

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

b) Each certification or audit report provided must: (i) identify the legal business name of the Contractor or applicable Sub-processor; (ii) identify the Contractor's or Sub-processor's certification date and the status of that certification; (iii) identify the services included within the scope of the certification report. If the carved-out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

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

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

e) The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, ISO 27018 and SOC 2 Type II for the period of the Contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

5.1.3 Cloud Service Provider (CSP) IT Security Assessment Program

a) If during the period of the Contract and following the approval of the Project Authority, the Contractor migrates the application and/or data from an on premise to a Cloud-based solution, the Contractor must demonstrate that the Cloud Service Provider:

[19] https://www.iso.org/standard/54534.html

[20] https://www.iso.org/standard/43757.html

[21] https://www.iso.org/standard/76559.html

i) Is compliant with the security requirements selected in the Government of Canada Security Control Profile for Cloud-Based Services for GC Services[22] for Cloud Services that are leveraged for the NCS; and

ii) Has been assessed under the Canadian Centre for Cyber Security (CCCS) CSP Information Technology (IT) Security Assessment Process (ITSM.50.100)[23].

b) Any Cloud Service Provider that has participated in the process must provide documentation to confirm that they have completed the onboarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS.

5.1.4 Supply Chain Risk Management

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

b) The Contractor must maintain a Supply Chain Risk Management (SCRM) Plan that describes the Contractor's approach to SCRM and demonstrates how the Contractor's approach will reduce and mitigate supply chain risks.

c) The supply chain risk management approach must continue to be aligned with one of the following best practices:

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

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

5.2 Conformance Review

a) Canada will—on an annual basis—conduct a GC-approved audit and conformance review—paid for by the Contractor—that includes but is not limited to:

i) Ensuring that the Solution conforms to the NCS Security Requirements (see Appendix E - Security Requirements Traceability Matrix) and the RCMP Departmental Security Control Profile (DSCP) including a review of the Plan of Action and Milestones to ensure milestones are being reached;

ii) Ensuring that all Solution software has current and up-to-date security updates and patches for all known vulnerabilities;

iii) Ensuring that the Contractor is proactively monitoring for software vulnerabilities in NCS and implementing any required security patches and software releases to remedy such vulnerabilities; and

iv) Composition of Contractor's core team.

---

[22] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html

[23] https://cyber.gc.ca/sites/default/files/publications/itsm.50.100-en.pdf

b) The Contractor must provide supporting evidence within ten (10) working days of a request by Canada, for any supporting evidence required for the conformance review.

c) If Canada deems that the supporting evidence does not support the conformity to the Contract, Canada will request a Plan from the Contractor to address the discrepancies identified by Canada with conformity to the terms and conditions of the Contract.

5.3 Security Validation

a) The Contractor must provide Canada with an SRTM that provides traceability for each NCS security assurance requirement marked for validation in the NCS Appendix E - Security Requirements Traceability Matrix). For each requirement, the SRTM must provide service documentation references within the service design specifications that describe the security safeguards to be implemented. The SRTM establishes assurance that the Solution design fully satisfies its security requirements.

b) All service documentation referenced in the SRTM must be provided to Canada with the SRTM and must describe the security safeguards in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements marked for validation in the NCS Appendix E - Security Requirements Traceability Matrix.

c) The Contractor must work collaboratively with the RCMP to assess the Solution against the RCMP DSCP via the SA&A process.

5.4 Security of Environment Systems and Data

5.4.1 Facility Security Clearance

a) The Contractor must, at all times during the performance of the Work, hold a valid Facility Security Clearance (FSC) to a Protected B level for all primary and secondary and Disaster Recovery sites hosting, storing or processing NCS data, in accordance with the Government of Canada Directive on Security Management[24].

5.4.1.1 Physical Security

a) The Contractor must maintain Physical Security measures for the protection of IT facilities and information system assets on which NCS data is stored and processed against all forms of unauthorized access, tampering, loss, damage, and seizure, and that is based on a prevent-detect-respond-recover approach to physical security. At a minimum, this must include:

i) Sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed service level agreement;

ii) Proper handling of IT media;

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

[24] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C

iv) Controlled access to information system output and storage devices to prevent unauthorized access to Canada's data;

v) Limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification;

vi) Escorting visitors and monitoring visitor activity;

vii) Maintaining audit logs of physical access;

viii) Controlling and managing physical access devices;

ix) Enforcing safeguarding measures for NCS data at alternate work sites (e.g. telework sites); and

x) Recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.

Reference: Government of Canada Directive on Security Management[25].

b) The Contractor's facilities must have physical protection measures that must be applied in accordance with practices in the Royal Canadian Mounted Police (RCMP) guidance and standards on physical security - G1-025 Protection, Detection and Response[26].

c) The Contractor must notify the Project Authority and the Industrial Personnel Security Services Directorate (formerly CISD) of any enhancements or changes made to the facilities managing the NCS.

5.4.2 Security Zoning

a) The Contractor must utilize security controls to ensure appropriate isolation of resources such that NCS data is not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Service's functionality and system administration. This includes access controls and enforcement of appropriate logical or physical segregation to support:

i) Separation between the Contractor's internal administration from resources used by its customers; and

ii) Separation of customer resources in multi-tenant environments in order to minimize one malicious or compromised consumer from affecting the service or data of another.

b) The Contractor must maintain Network security zoning aligned with:

i) Canadian Security Establishment (CSE) IT Security Guidance (ITSG) ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada[27]; and

---

[25] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C

[26] http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-025-eng.htm

[27] https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22

ii) Canadian Security Establishment (CSE) Network Security Zoning - Design Considerations for Placement of Services within Zones (ITSG-38)[28].

c) The Contractor must monitor and maintain Network security zoning to ensure:

i) Strict control of all Public Zone interfaces, including all external uncontrolled networks such as the Internet, at a defined security perimeter; and

ii) Perimeter defence safeguards (e.g. firewalls, routers) which mediate all traffic and to protect servers that are accessible from the Internet.

d) Any planned or unplanned changes to the environment, throughout the period of the Contract, must be documented and updated in accordance with the Change Management Plan and Process.

5.4.3 Solution Design Review

a) The service design for the NCS must be reviewed and approved by Canada. This includes providing Canada with a copy of the proposed architecture of the NCS that will enable Canada to perform:

i) a review of the proposed security safeguards and security components that will be implemented as part of the NCS; and

ii) a review of the security configuration of all security devices.

5.4.4 Malware Protection

a) The Contractor must protect IT components used to deliver and manage the solution from cyber threats, including monitoring devices, servers, peripheral devices, and desktop workstations, and must protect and prevent penetration by external sources;

b) The network protection must be implemented and maintained to detect and eliminate malicious software and/or unauthorized external connection attempts on the network; and

c) The Contractor must scan the Contractor environment supporting the NCS for the presence of malware. There must be active host-protection mechanisms on servers that performs:

i) On access scans for malware; and

ii) Scheduled active scanning of malware at a minimum of once a month.

5.4.5 Security Updates

a) The Contractor must apply Security Updates on regular Operating Systems and Applications to patch vulnerabilities utilizing a risk based approach aligned to the methodology set out in Canadian Security Establishment (CSE) Security Vulnerabilities and Patches Explained - IT Security Bulletin for the Government of Canada (ITSB-96)[29].

5.4.6 Patch and Vulnerability Management

a) The Contractor must perform patch management including, at a minimum:

---

[28] https://www.cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38

[29] https://cyber.gc.ca/en/guidance/security-vulnerabilities-and-patches-explained-it-security-bulletin-government-canada-itsb

i) Ensuring a current supported version of applications and operating systems are used;

ii) Ensuring that vulnerabilities are evaluated, and vendor-supplied security patches are applied in a timely manner;

iii) Prioritizing critical patches and service packs using a risk- based approach; and

iv) Testing and verifying to ensure that patches have been implemented properly.

5.4.7 Privilege Management

a) The Contractor must manage and monitor privileged access to the NCS to ensure that all service interfaces are protected from unauthorized access. This process must include, at a minimum:

i) Enforce and audit authorizations for access to NCS data;

ii) Restrict and minimize access to only authorized devices, users, and administrators with an explicit need to have access;

iii) Constrain all access to service interfaces that host NCS data to uniquely identified, authenticated and authorized individuals;

iv) Implement multi-factor authentication mechanisms to authenticate users with privileged access;

v) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to NCS data;

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

vii) Adhere to the principles of least privilege and need-to-know when granting access to employees and contractors;

viii) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of services and infrastructure;

ix) Implement an automated or manual process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions. If a manual audit process is used, a policy or procedure for this activity must be documented and shared with Canada; and

x) Upon termination of employment or contract, terminate or revoke authenticators and access credentials associated with the employee or subcontractor.

5.4.8 Secure Data Migration and Exchange

a) The Contractor must maintain data migration practices to support implementation of the NCS as follows:

i) **Between the Contractor and their subcontractors**

The Contractor must leverage the Government of Canada approved Managed Secure File Transfer (MSFT)[30] solution for Secure Data Migration and Exchange between themselves and their subcontractors (if applicable) that supports Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol over Secure Socket Layer (FTPS) and File Transfer Protocol over Secure Shell (SFTP) and provide data encryption compliant to the Federal Information Processing Standards (FIPS) 140-2 cryptography requirements.

ii) **Between the Contractor and Canada**

The Contractor must establish secure network connections that implement TLS 1.2, or subsequent versions, and uses supported cryptographic algorithms and certificates, accepted by the CSE as follows:

- Canadian Security Establishment (CSE) Guidance on Securely Configuring Network Protocols (ITSP.40.062)[31] Section 3.1 for AES cipher suites
- Canadian Security Establishment (CSE) Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information (ITSP.40.111)[32]

The Contractor must update its secure network connection in accordance with the above CSE requirements as those CSE requirements evolve during the period of the Contract.

iii) **Between the Contractor and third party**

Upon the Project Authority Approval and Personnel Security Screening Division (PSSD) (formerly CISD) clearance, the Contractor must provide a Secure data transfer tool or methodology that allows the Contractor to transfer data to an approved third party to facilitate external audits and other Government initiated projects.

5.4.9 Cryptographic Protection

a) The Contractor must use, and update if deemed necessary in discussion with Canada, cryptography protection to maintain confidentiality or integrity safeguards or as part of the authentication mechanism (e.g. VPN solutions, TLS, software modules, PKI, and authentication tokens, where applicable) in use for the Service.

b) The Contractor must use the following approved cryptographic algorithms and cryptographic key sizes and crypto periods:

i) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSE and validated by the NIST Cryptographic Algorithm Validation Program[33] and are specified in ITSB-111 or in a subsequent version; and

---

[30] http://sftweb.pwgsc.gc.ca/sft-html/Documents_e.html

[31] https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062

[32] https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111

[33] https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

ii) Be implemented and operated in an approved mode in a Cryptographic Module, validated by the NIST Cryptographic Module Validation Program[34] to at least NIST Security Requirements for Cryptographic Modules (FIPS 140-2)[35] validation at Level 1. At a minimum, FIPS 140 compliant/validated cryptography must be employed at perimeter protection devices or anywhere else encryption is required.

5.4.10 Security of Electronic Data Interchange

a) The Contractor must ensure that NCS data submitted or exchanged between the NC3 and Partners via EDI or other Digital Services comply with all established NCS security requirements;

b) The Contractor's Solution must facilitate secure transmission of information using EDI between Partners and the NC3;

c) The Contractor's Solution must safeguard the integrity and authenticity of all NCS data at rest and in transit, from corruption and inadvertent or malicious changes by employing hashing, digital certificates, or similar technology, in accordance with 5.4.10 Cryptographic Protection; and

d) The Contractor must ensure that security and privacy of information is maintained throughout any data conversion or loading exercise.

5.4.11 Data Storage and Retention

a) The Contractor must store all NCS back-up data in accordance with NC3 Information retention requirements and the following:

i) All handling of any removable media that may be used with the system must meet with the requirements for proper labelling, destruction and handling, and storage of these types of assets in accordance with Secure use of portable data storage devices within the Government of Canada Secure use of portable data storage devices within the Government of Canada (ITPIN 2014-01)[36];

ii) All back-up data must be stored in a secure, fire and flood protected area;

iii) Data storage protection must meet Advanced Encryption Standards (AES), with key lengths of 128 bits, to protect the confidentiality and integrity of backup information at the storage location;

iv) The Contractor must assess the viability of whether storage media can be securely reused based on the CSE Guidelines on IT Media Sanitation (ITSP.40.006)[37]; and

v) The Contractor must pay for any costs associated with the destruction of data initiated by the Contractor and approved by the Project Authority.

---

[34] https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

[35] https://csrc.nist.gov/publications/detail/fips/140/2/final

[36] https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/policy-implementation-notices/secure-use-portable-data-storage-devices-government.html

[37] https://www.cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006

5.4.12 Data Extraction

a) The Contractor must provide the tools and services that allow Canada to:

i) Extract all online, near line, and offline Canada's data, including, at a minimum, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a Canada code repository, and network configurations such that any Canada End User can use these instructions to migrate from one environment to another environment; and

ii) Securely transfer all Canada's data, including content data and associated metadata, in a machine-readable and usable format, including CSV format, and in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value[38].

5.4.13 Data Destruction

a) At the end of the contract period (i.e. at contract expiration or termination) or upon request by the Project Authority, the Contractor must follow the CSE Guidelines on IT Media Sanitation (ITSP.40.006)[39] that contained NCS data;

b) The Contractor must provide reported evidence, such as a certificate, to attest to the destruction of all user data related to the NCS; and

c) All costs associated with the destruction of media that contained or hosted NCS Protected B Information is to be borne by the Contractor.

5.4.14 Data Transportation

a) In the event that data on paper must be physically transported, the Contractor must adhere to RCMP G1-009 Transport and Transmittal of Protected and Classified Information[40] and the Contract Security Manual[41] – Chapter 6: Handling and safeguarding of classified and protected information and assets;

b) The Contractor must mark all hard copy documents and other media with the highest appropriate security classification as provided by the Project Authority; and

c) The Contractor must obtain Project Authority approval prior to moving data in or out of Protected B physical domain.

---

[38] https://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/Pages/guidelines-file-formats-transferring-information-resources-enduring-value.aspx

[39] https://www.cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006

[40] https://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-eng.htm

[41] https://www.tpsgc-pwgsc.gc.ca/esc-src/msc-csm/chap6-eng.html

5.5 Secure Access Controls

5.5.1 Personnel Security Clearance

a) The Contractor must ensure that all individuals handling, viewing, managing, or who may come in contact with, NCS data or who have access to the NCS designated facilities, have a valid security clearance at the level of Reliability or higher based on the levels of security requirements as per Government of Canada Levels of security[42]. The Contractor must ensure that any new personnel including subcontractors have appropriate clearances and that clearances are maintained throughout the period of the Contract; and

b) The Contractor must ensure personnel screening measures are applied in accordance with the definition and practices in the Government of Canada's Standard on Security Screening[43] to ensure the adequate protection of Protected B Information.

5.5.2 Access Controls

a) The Contractor must provide role-based access control as follows:

   i) The Contractor must implement Access Controls based on roles defined in the NCS, where each role is assigned capabilities and access according to the least privilege required for that role, and a need-to-know;

   ii) The Contractor must implement a process to manage a unique user account for each of the Project Authority identified users of the NCS solution Protected B data, including at a minimum, the Police and Partner Portal (P3) and NCS Interfaces; and

   iii) The Contractor must apply identified changes to user access profiles within three Days of receipt of information from the Project Authority;

b) The Contractor must implement multi-factor authentication mechanisms for users and privileged accounts;

c) The Contractor must ensure passwords comply with CSE's User Authentication Guidance for Information Technology Systems (ITSP.30.031)[44];

d) The NCS solution should notify users, upon successful logon, of the date and time of the last successful logon;

e) Any change to a user account must be accompanied by an audit record indicating what was changed, which user account made the change, on what date and time and by whom;

f) The Contractor must ensure Contractor user access and controls are kept current with all changes or updates to Contractor staff and also provide notification of such changes to the Project Authority.

5.5.3 Account Protection

a) The Contractor must maintain controls to issue and update existing account passwords in accordance with either:

---

[42] https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html

[43] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115

[44] https://www.cse-cst.gc.ca/en/node/2454/html/28582

i) CSE's User Authentication Guidance for Information Technology Systems (ITSP.30.031)[45]; or

ii) Other industry best practices such as ISO 27001 or NIST.

5.5.4 Security Awareness and Training

a) The Contractor must provide a security awareness training or briefing session to ensure that all personnel including subcontractors handling NCS Protected B Information understand their role and responsibilities in managing information security, prior to commencing work on the NCS.

5.6 Security Testing

a) The Contractor must provide Canada with a Security Testing Plan that documents the test cases to verify each NCS Production Environment (NCS-PE) security assurance requirement, marked for Security Testing in the Appendix E - Security Requirements Traceability Matrix).

b) The Contractor must perform the Security Testing Plan for each security safeguard and provide Canada with a Security Testing Report that satisfies one or more of the security requirements marked for security testing in Appendix E - Security Requirements Traceability Matrix:

i) The Security Testing procedure must confirm that the security safeguard is implemented correctly and satisfies applicable standards as specified in the service design specifications;

ii) The expected and actual results for each Security Testing procedure;

iii) For each deviation from the expected result that could be corrected at the time of verification, a description of the corrective measure(s) that were implemented in the NCS-PE; and

iv) For each deviation from the expected result that could not be corrected at the time of verification (e.g., due to more significant changes), a Change Request reference.

c) The Contractor must update the SRTM to include the tracing between the security requirements marked for Security Testing and the Security Testing procedures.

d) The Contractor must allow Canada to witness the Security Testing that includes the ability to observe Contractor representatives while they execute the Security Testing procedures or the ability to observe the test log results where the security testing is automated.

5.7 Security Controls Assessment Methods

a) The Contractor must use the following Security Controls Assessment Methods in the Security Test and Evaluation Report:

i) ASSESSMENT METHOD: Examine:

(1) ASSESSMENT OBJECTS:

[45] https://www.cse-cst.gc.ca/en/node/2454/html/28582

a) Specifications (e.g., policies, plans, procedures, system requirements, designs);

b) Mechanisms (e.g., functionality implemented in hardware, software, firmware); and

c) Activities (e.g., system operations, administration, management; exercises).

(2) DEFINITION: The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time; and

ii) ASSESSMENT METHOD: Test:

(1) ASSESSMENT OBJECTS:

a) Mechanisms (e.g., hardware, software, firmware); and

b) Activities (e.g., system operations, administration, management; exercises).

(2) DEFINITION: The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

5.8 Vulnerability Assessment

a) The Contractor must allow Internal Vulnerability Assessment testing to be conducted on an as and when required basis by Canada, the Contractor, or a third party selected by Canada or the Contractor. This testing must be conducted at a minimum on a yearly basis and aligned to the Vulnerability Management controls in the DSCP. The Contractor must determine the assignment of responsibility for supporting Vulnerability Assessment testing.

b) If the Contractor selects to allow Canada to perform the Internal Vulnerability Assessment testing, the Contractor must provide:

i) Logical access to the RCMP Protected B Cloud Tenant subscription where the NCS Test Environment (NCS-TE) infrastructure is located and operated;

ii) Network access or accesses to the NCS-TE to allow for the scanning of network and host devices; and

iii) Assistance for the duration of any portion of the Internal Vulnerability Assessment of at least one (1) technical resource who is familiar with the technical aspects of the NCS-TE (i.e., the software and network products and their configuration).

c) If the Contractor (or third party on behalf of the Contractor) chooses to conduct its own Internal Vulnerability Assessment testing, the Contractor must:

i) Submit a Vulnerability Assessment Plan to Canada for its prior approval;

ii) Include within the scope of the plan, the scanning of all network and host devices deployed in the NCS-TE;

iii) Conduct the vulnerability assessment testing in the NCS-TE; and

iv) Provide the results to Canada for review and analysis. Canada may require implementation of Contractor-initiated changes based on review and analysis.

d) Canada may conduct External Vulnerability Assessment testing against the NCS-TE and provide a Vulnerability Assessment Report to the Contractor that will identify the vulnerabilities that were detected by Canada.

e) The Contractor must provide Canada with a Vulnerability Mitigation Report that includes:

i) A list of vulnerabilities for which Canada is recommending the implementation of corrective measures;

ii) A list of vulnerabilities for which the Contractor is recommending the implementation of corrective measures if the Contractor has chosen to conduct its own Internal Vulnerability Assessment testing;

iii) A description of the corrective measures to be implemented including expected time frames; and

iv) Service documentation referenced in the SRTM that must be updated as a result of the implementation of the corrective measures.

f) The Contractor must implement the corrective measures identified in the approved Vulnerability Mitigation Report within the time frame established in the Vulnerability Mitigation Report.

6. Project Management

6.1 Background

a) Currently Canada uses a project management methodology that conforms to the Government of Canada's Directive on the Management of Projects and Programmes (effective April 2019)[46].

b) Canada will manage the delivery of the NCS Project using a hybrid project management approach that integrates Agile methods with the existing RCMP project management methodology. Notional baselines for the project scope, schedule and cost will be defined with enough flexibility to accommodate the Contractor's iterative and dynamic development principles. These notional baselines will the basis to monitor progress, measure performance, and initiate any corrective action.

6.2 Approach to Managing Solution Delivery

a) Canada expects that the Contractor's system development and integration methods embrace interactions between the Contractor and the RCMP Business Client who owns and maintains the Product Backlog. The RCMP Business Client may reprioritize the content of the Product Backlog as they see fit.

b) The Contractor must work with the RCMP Business Client to identify the highest ranked functionalities at the beginning of each sprint (incremental releases or delivery of functionality), along with any details needed for the Contractor to implement those functionalities. The Contractor must estimate the work and commit to only what can be done in the sprint. Changes will be allowed during the sprint only if approved by Canada through the formal change authorization process. While the sprint features are being developed for delivery, the RCMP Business Client in conjunction with the Contractor will select the next set of features for the next sprint.

c) Any significant changes or deletion of a must have scope must proceed through formal change authorizations, in accordance with the approved change management process described in the Contractor Project Management Plan deliverable.

d) Activities for the NCS project must be sequenced and product features will be ranked according to the RCMP Business Client needs and priorities. It is expected that features of the Solution will be developed through multiple sprints in which teams execute tasks that can be completed within a set time.

e) Releases and sprints must continuously develop features listed in Product Backlog that have been prioritized in collaboration with the business client until the Full Operating Capability is achieved at the end of the Contract.

f) Overall project progress and performance will be reviewed through scheduled checkpoints, with a larger audience to solicit concerns, check performance data (e.g., progress toward achieving desired outcomes), and correct course, as necessary.

g) Releasing improvements are not constrained by a schedule. Improvements may happen as often as possible so that the business client and other users receive maximum benefit. By releasing small updates frequently, the team can be more confident that the changes that they make do not negatively impact the system's performance or its achievement of outcomes.

---

[46] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32594

6.3 Schedule Management Requirements

a) The Contractor must manage and be accountable for the project schedule throughout all the stages of the Contract life cycle as the success of the project depends heavily on having an integrated and reliable schedule that defines when work will occur and how project activities are interrelated.

b) The Contractor project schedule must describe a roadmap with the must have Business Capabilities based on the prioritization of deliverables communicated by the Business Client and reflected in this SOW.

c) The Contractor must use its own metrics to measure progress and estimate the remaining effort. At the end of each sprint, the Contractor must analyze progress data to determine if the tasks' level of effort were underestimated or overestimated allowing for more accurate planning of subsequent sprints.

6.4 Planning and Control Framework

a) The Contractor must maintain a planning and control framework for the duration of the Contract. The Contract deliverables must be executed, delivered, and updated in accordance with the delivery schedule identified herein and further, refined in the Contractor's proposed project schedule.

6.5 Project Management Plan

a) The Contractor must deliver a Project Management Plan that describes the processes that the Contractor will use to ensure that the Contract and the delivery of the Solution are being executed in accordance with the terms and conditions of the Contract and established government policies and industry standards for the management of projects.

b) The Contractor must also describe their risk management plan, indicating how it intends to identify, mitigate, manage, and report risks during Contract execution.

c) The Contractor must also describe their issue management plan, providing details of the processes and procedures by which issues related to the execution of the Contract will be escalated to higher authority for decision and resolution.

d) The Contractor must describe its change management process to indicate its approach and procedures in handling, authorizing and managing changes to the requirements, scope, schedule, and cost during Contract execution.

e) The Contractor must utilize configuration management processes to provide Canada with timely notification of any interruption that is expected to impact service availability and performance per requirements included in Section 3.18 – Performance Metrics and Section 3.15 – Solution Availability and Performance.

f) The Contractor must indicate how they will address stakeholder engagement and communication. This includes, identifying stakeholders, analyzing stakeholders to determine influence and interest in the execution of the Contract, defining approaches for engaging with stakeholders, roles, and responsibilities for the stakeholders' engagement process.

g) The Contractor may decide on content and format for this deliverable and the number of artifacts (e.g., diagram, views, models, and matrices) that they may provide. Artifacts submitted must be clear and concise, well-described, and allow Canada to understand how the requirements are being met.

6.6 Project Resources

6.6.1 Senior Contractor Project Manager

a) The Contractor must appoint a Senior Contract Project Manager (CPM).

b) The Senior CPM must perform the day to day management and coordination of the Contract and must be the point of contact within the Contractor's Organization for the delivery of goods and services associated with the Contract.

c) The Senior CPM must have previous experience managing Canadian Federal Government IM/IT projects valued at more than CAN$10.0M.

6.6.2 Technical Resources

a) In addition to the core Contract resources included within the implementation (for example the Senior CPM), Canada may require from the Contractor ad-hoc services, for instance technical support. The Contractor must provide these optional professional service resources on an as-and-when requested basis via Task Authorizations.

b) The Contractor must commit to the availability of those technical resources to provide those services.

7. Phase 2 Deliverables

7.1 Overview

a) The Contractor must deliver a fully functional Solution and provide for on-going support including:

   i) Project management;

   ii) System design configurations;

   iii) Deployment;

   iv) Documentation;

   v) Testing;

   vi) User Support;

   vii) Providing in-depth as-and-when requested consultation regarding best practices and process efficiencies, ensuring a successful integration with the Technical Authority environment existing processes, procedures and technology environment;

   viii) Providing as-and-when requested required training and training materials for Power-Users users, SMEs, end users and technical support personnel; and

   ix) Providing support to ensure the RCMP maximizes the flexibility and cost effectiveness of the Solution.

b) To ensure the success of the implementation of the Solution, the project will include, at minimum, the following implementation deliverables. The creation of each deliverable is the responsibility of the Contractor and must be formally presented to the Technical Authority for review and acceptance. For milestones with multiple stages, each stage is expected to contain each deliverable (unless noted otherwise).

c) The Contractor must use Canada-approved Microsoft Office applications (Word, Excel, PowerPoint, Visio, and Project) to create and update deliverables. All documents must be fully editable so they can be updated by Canada. Should the Contractor wish to submit documents in other softcopy formats, this request must be expressly authorized by Canada.

d) Phase 2 Implementation commences on the date that Canada exercises its option to the Contractor to deliver Phase 2 – Full Solution, and must be completed within approximately 17 months of the date that Canada exercises its option to deliver Phase 2.

7.2 List of Phase 2 Deliverables

a) The Contractor must provide the following deliverables:

   i) **Phase 2 Kick-off Meeting** which must be scheduled within one (1) week from the date of Phase 2 work Option exercised by Canada and which must:

      (1) Discuss the overall Phase 2 approach and methodology, Contract, working relationships, timeframe, risks and issues;

      (2) The Chairperson for the kick-off meeting must be the PSPC Contracting Authority;

(3) Include an agenda and a presentation, if applicable, that would be submitted within a reasonable delay prior to the start date of the meeting; and

(4) Include minutes of the kick-off meeting to be provided to the Contracting Authority for approval, prior to distribution to all Authorities.

ii) **Phase 2 Schedule** which must include:

(1) The scope of the Phase 2 work including expected milestones, deliverables, dependencies, Iterations / Sprints based on Business Capabilities (NCS BCM) priorities to be delivered under this Statement of Work (SOW);

(2) Implementation timeline; and

(3) Subject to approval by the RCMP Technical Authority with the understanding that specifics of the Schedule may change over the course of Phase 2 if collaboratively decided by RCMP and the Contractor to be in the best interest of the project.

iii) **Project Management Plan** for Phase 2 Work (See Section 6.5 – Project Management Plan), which must include but not be limited to:

(1) Executive Summary – Describe at a high level, the key elements of the project that are detailed throughout the project management plan;

(2) Project Governance – Describe the project governance including the key project team members' roles and responsibilities;

(3) Development Methodology – Describe the methodology that will be used to manage the software solution development and integration process;

(4) Project Management Methodology – Describe the approach that will be used to manage the project;

(5) Project Scope – There should be definition as to the scope of phase 2 as well as the major deliverables. Project assumptions should also be included, clarifying grey areas in the project scope;

(6) Constraints – a list of any known project execution constraints;

(7) Dependencies – a list of known project dependencies;

(8) Risk Management – Detail the process to be employed on the project in order to manage risk;

(9) Issue Management – Define the process to be used to manage issues identified on the project;

(10) Change Management – Describe the change management process to be utilised on the project; and

(11) Stakeholder engagement and communication.

iv) **Progress Reports**, which must:

(1) Be provided to the RCMP Technical Authority on a semi-monthly basis: on the 15th and on the last day of the month;

(2) Describe the Contractor's progress in relation to the project baselines as defined and approved in the Phase 2 Schedule deliverable;

(3) Identify the areas of risks, slippages, the project critical path, and problems areas;

(4) Identify issues requiring mitigation, decisions, or resolution; and

(5) Include an executive project dashboard that captures in a graphical manner, the highlights of the various parameters (e.g., scope, cost, schedule, risks, and issues) associated with the execution of the Contract.

v) **Progress Review Meetings**, which must:

(1) Be held on a semi-monthly basis;

(2) Be chaired by the RCMP Technical Authority;

(3) Meet government guidelines on COVID-19 for gathering and social distancing;

(4) Be conducted in accordance with the Progress Review Meeting (PRM) agenda to be provided by the Contractor;

(5) Include the minutes of the PRMs. These minutes must include the records of decisions, action items and any other points of discussion as covered in the PRM. These minutes must be delivered to Canada three (3) business days after the PRM; and

(6) In addition to the scheduled PRMs, Canada—at its sole discretion—may call upon the Contractor to provide representation at ad-hoc meetings. These ad-hoc meetings are intended to address matters of a serious nature that cannot reasonably be delayed until the next progress review meeting.

vi) **Solution Implementation Plan** for Phase 2 work that must include:

(1) The Contractor must demonstrate that all technical and business capabilities have been accounted for in the implementation plan, with the understanding that the priority and specifics of individual capabilities will be determined collaboratively over the course of Phase 2 by RCMP and the Contractor.

(2) The implementation plan must contain, at a minimum, the following components:

a) A description of the iterative approach and methodology that the Contractor will use to configure, integrate and release the Solution, including how COVID-19 challenges will be addressed;

b) A description of the planned iterative deployment (Incremental releases), installation, and implementation milestones over the duration of the contract;

c) A detailed step by step set of instructions (i.e., installation manual) that is clear, accurate, and sufficiently detailed to enable Canada to install applicable components of the Solution in the RCMP Protected B Cloud Tenant;

d) List of Infrastructure and Software Licenses for the Solution;

e) A detailed list of resources that will be hosted in the RCMP Protected B Cloud Tenant in order to provision, operate, and scale the Solution;

f) The data model must include a correlation between the sizes such as SKU of the resource in a scalable scenario;

g) A technical description of the packaging or distribution method or installation archive for each of the infrastructure components and software components used in the Solution. Hypothetical examples could be: Docker images, Terraform scripts, Linux Binaries, WebArchives, and Windows Software;

h) A technical description of any and all technologies and services required to develop, implement, operate, and maintain the Solution through. Hypothetical examples: Jenkins, Jira, apt-get, Trello, Git-Lab;

i) A description of configuration and version control tools and processes that will be put in place to manage iterative deployments; and

j) A description of the Solution Cloud Service Delivery Model describing how the Solution is deployed (internal to the RCMP (IaaS or Private PaaS on an RCMP Protected B cloud tenant) with the grant of perpetual licenses; as a Software as a Service (SaaS) or Public PaaS; or a combination of SaaS and Perpetual Licenses referred to as a "Hybrid").

(3) The Contractor may decide the best format and number of artifacts (e.g., diagram, views, models, matrices) that are required. Artifacts submitted must be clear and concise, well-described, and allow the Technical Authority to understand how the requirements are being met.

vii) **Security Management Plan** that must describe:

(1) The security controls to be implemented and monitored based on the Contractor's security assessment;

(2) The Contractor's roles and responsibilities for security;

(3) The process to identify, report and respond to security incidents; and

(4) The security hardening of systems including ongoing patch management.

viii) **Disaster Recovery Plan (DRP)** that must document and describe:

(1) A structured approach as to how the RCMP can quickly resume work after an unplanned incident involving the Solution, including:

a) establishing the range or extent of necessary treatment and activity - the scope of recovery;

b) gathering relevant network infrastructure documents; and

c) identifying the most serious threats and vulnerabilities, and the most critical assets;

(2) Procedures for updating the DRP and implementing a DRP audit;

(3) Procedures to help the RCMP resolve data loss and recover system functionality so that it can perform in the aftermath of an incident, even if it operates at a minimal level; and

(4) See Section 3.6 - 3.6 – Disaster Recovery Plan of this SOW for further details.

ix) **Backup and Recovery Plan** that describes at a minimum;

(1) Procedures;

(2) Roles and Responsibilities;

(3) Verification and test processes;

(4) Error notification processes; and

(5) Restoration processes.

x) **Information Technology Continuity Plan**

(1) Describe at a minimum; Invocation procedures, assessment and escalation procedures, roles and responsibilities, incident logs, fall-back procedures and service recovery procedures through to normal service delivery.

xi) **System Architecture**

(1) Describe the components and features that the Contractor will deliver and a timeline of when these components will be included in the Solution architecture; and

(2) Provide the System Architecture.

xii) **System Design Document**

(1) See Section 3.5 – Solution Technical Documentation of this SOW for details.

xiii) **System Security Plan**

(1) In accordance with the deliverables described in Section 5 – System Security Plan of this SOW.

xiv) **Security Assessment and Authorization** (SA&A)

(1) In accordance with the details provided in Section 3.5 – Solution Technical Documentation of this SOW.

xv) **Physical Data Model**

(1) Provide a Physical Data Model of the Solution repository.

xvi) **Information Life Cycle Plan**

(1) Describing the complete data management lifecycle (collection to disposal) including the processes in place to manage data that has reached end of retention time limits.

xvii) **Training Plan**

(1) Describing how the Contractor plans to offer initial and updated bilingual (English and French) training resources.

(2) See Section 3.10.1 – Training Plan of this SOW for further details.

xviii) **Training Materials**

(1) Must be provided in English and French, and include electronic copies of operating manuals, technical manuals, and other user documentation that is required to learn, use, and maintain the Solution.

(2) See of this SOW for further details.

xix) **Training Delivery**

(1) Must be provided in English and French.

(2) See Section 3.10.3 – Training Delivery of this SOW for further details.

xx) **Solution Acceptance Test Plan** which must include:

(1) A description of the planning and testing that will be undertaken for the Prototype Solution;

(2) A description of the general acceptance procedures for the planning, preparation, and completion of the tests; and

(3) See Section 3.7 – Solution Acceptance Test Plan of this SOW for further details.

xxi) **Solution Acceptance Test Report** which must include:

(1) The results of acceptance tests performed on the Solution, -in accordance with the Solution Acceptance Test Plan;

(2) Confirmation that the Solution has passed all the required acceptance tests and meets the requirements as stated in the Contract or that the Solution has failed the acceptance tests with reasons for failure; and

(3) See Section 3.8 – Solution Acceptance Test Report of this SOW for further details.

xxii) **NCS and Documentation**

(1) Include incremental releases of the Solution until full operating capability is delivered.

(2) See Section 3.44 – Software Solution and Documentation of this SOW for further details.

xxiii) **Transition Plan**

(1) In accordance with details provided in Section 3.12 – Transition Plan of this SOW.

xxiv) Transition Out Plan

(1) In accordance with details provided in Section 3.13 Transition Out Plan of this SOW.

xxv) **Professional Services and Training Services**

(1) To be provided, on an as needed basis, for solution implementation, data migration, and other specialized services.

xxvi) **Project Close-Out Report** to mark the completion of the project by:

(1) Assessing the project's performance and outcomes, identifying the lessons learned, and confirming that essential contractual and other project close-out activities have been completed;

(2) Complete the transfer of assets, deliverables, and all ongoing administrative functions to the RCMP in service organization and

(3) The Contractor may decide the best format and number of artifacts (e.g., diagram, views, models, matrices) that are required. Artifacts submitted must be clear and concise, well-described, and allow the Technical Authority to understand how the requirements are being met.

7.3 Phase 2 Deliverables Schedule

a) The following table identifies the Contract deliverables for Phase 2 and delivery dates. The deliverables must be submitted to the Technical Authority in the format and by the delivery dates specified. All days listed in the deliverable table are business days.

Table 7-1: List and Schedule of Contract Deliverables

#	Description	Delivery Date
1.	Phase 2 Kick-off Meeting	1 week from Phase 2 Option exercised date
2.	Phase 2 Schedule, digital copy delivered to Client Technical Authority	2 weeks from Phase 2 Option exercised date
3.	Project Management Plan, digital copy delivered to Client Technical Authority	3 weeks from C Phase 2 Option exercised date
4.	Progress Reports, digital copy delivered to Client Technical Authority	Semi-Monthly from Phase 2 Option exercised date
5.	Progress Review Meetings	Semi-Monthly from Phase 2 Option exercised date
6.	Final Solution Implementation Plan, digital copy delivered to Client Technical Authority	4 weeks from Phase 2 Option exercised date
7.	Security Management Plan, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
8.	Disaster Recovery Plan, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
9.	Backup and Recovery Plan, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
10.	Information Technology Continuity Plan, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable

Table 7-1: List and Schedule of Contract Deliverables

#	Description	Delivery Date
11.	System Architecture, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
12.	System Design Document, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
13.	System Security Plan, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
14.	Security Assessment and Authorization	As depicted in Contractor Phase 2 Schedule Deliverable
15.	Physical Data Model, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
16.	Information Life Cycle Plan, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
17.	Training Plan, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
18.	Training Materials, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
19.	Training Delivery	As depicted in Contractor Phase 2 Schedule Deliverable
20.	Solution Acceptance Test Plan, digital copy delivered to Client Technical Authority	5 weeks from Phase 2 Option exercised date
21.	Solution Acceptance Test Report, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
22.	NCS and Documentation – Multiple Releases	As depicted in Contractor Phase 2 Schedule Deliverable
23.	Transition Plan, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable
24.	Transition Out Plan	As depicted in Contractor Phase 2 Schedule Deliverable
25.	Professional Services and Training Services	As and when requested
26.	Project Closeout Report, digital copy delivered to Client Technical Authority	As depicted in Contractor Phase 2 Schedule Deliverable

8. Reference Documents

a) Access to Information Act: https://laws-lois.justice.gc.ca/eng/acts/a-1/

b) Canadian Centre for Cyber Security - Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22): https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22

c) Canadian Centre for Cyber Security – Cloud Service Provider (CSP) Information Technology Security (ITS) Assessment Process: https://cyber.gc.ca/sites/default/files/publications/itsm.50.100-en.pdf

d) Canadian Centre for Cyber Security - Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111): https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111

e) Canadian Centre for Cyber Security – Guidance on Securely Configuring Network Protocols (ITSP.40.062): https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062

f) Canadian Centre for Cyber Security – IT Media Sanitization (ITSP.40.006): https://www.cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006

g) Canadian Centre for Cyber Security – Network Security Zoning - Design Considerations for Placement of Services within Zones (ITSG-38): https://www.cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38

h) Canadian Centre for Cyber Security – Security Vulnerabilities and Patches Explained - IT Security Bulletin for the Government of Canada (ITSB-96): https://cyber.gc.ca/en/guidance/security-vulnerabilities-and-patches-explained-it-security-bulletin-government-canada-itsb

i) Canadian Centre for Cyber Security - User Authentication Guidance for Information Technology Systems (ITSP.30.031 v3): https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3

j) Canadian Security Establishment - User Authentication Guidance for Information Technology Systems: https://www.cse-cst.gc.ca/en/node/2454/html/28582

k) Government of Canada Enterprise Architecture/Standards: https://wiki.gccollab.ca/Government_of_Canada_Architectural_Standards

l) Government of Canada Cloud Brokering Services Catalogue: https://cloud-broker.canada.ca/s/pbmmcatalogpage?language=en_CA

m) Government of Canada Digital Standards: https://www.canada.ca/en/government/system/digital-government/government-canada-digital-standards.html

n) Government of Canada Guidelines on Responsible Use of Artificial Intelligence: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html

o) Government of Canada Secure use of portable data storage devices within the Government of Canada - Information Technology Policy Implementation Notice (ITPIN): https://www.canada.ca/en/government/system/digital-government/modern-

emerging-technologies/policy-implementation-notices/secure-use-portable-data-storage-devices-government.html

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

q) Government of Canada Standards on APIs: https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html

r) International Organization for Standardization (ISO) - Information technology — Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015): https://www.iso.org/standard/43757.html

s) International Organization for Standardization (ISO) - Information technology — Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2019): https://www.iso.org/standard/76559.html

t) International Organization for Standardization (ISO) - Information technology — Security techniques – Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013): https://www.iso.org/standard/54534.html

u) ITSG-33 - Information Technology Security Guidance - IT Security Rick Management: A Lifecycle Approach: https://cyber.gc.ca/en/guidance/annex-3a-security-control-catalogue-itsg-33

v) Library and Archives of Canada Act: https://laws-lois.justice.gc.ca/eng/acts/L-7.7/index.html

w) Library and Archives of Canada - Guidelines on File Formats for Transferring Information Resources of Enduring Value: https://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/Pages/guidelines-file-formats-transferring-information-resources-enduring-value.aspx

x) National Institute of Standards ND Technology (NIST) – Cryptographic Algorithm Validation Program: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

y) National Institute of Standards ND Technology (NIST) - Security Requirements for Cryptographic Modules (FIPS 140-2): https://csrc.nist.gov/publications/detail/fips/140/2/final

z) Official Languages Act: https://laws-lois.justice.gc.ca/eng/acts/o-3.01/

aa) Privacy Act: https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html

bb) Public Services and Procurement Canada - Managed Secure File Transfer – Documents: https://sftweb.pwgsc.gc.ca/sft-html/Documents_e.html

cc) Public Services and Procurement Canada - Request for Supply Arrangement (RFSA): https://www.tpsgc-pwgsc.gc.ca/app-acq/cral-sarc/saas-eng.html

dd) RCMP Departmental Security Control Profile: Available upon request from the Contract Authority

ee) RCMP G1-009 Transport and Transmittal of Protected and Classified Information: https://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/g1-009-eng.htm

ff) RCMP G1-025 Protection, Detection and Response: https://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-025-eng.htm

gg) Standard Acquisition Clauses and Conditions (SACC) 2003: https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manualconditions-manual

hh) Treasury Board of Canada Secretariat, Algorithmic Impact Assessment (AIA): https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html

ii) Treasury Board of Canada Secretariat, Chapter 6: Handling and safeguarding information and assets: https://www.tpsgc-pwgsc.gc.ca/esc-src/msc-csm/chap6-eng.html

jj) Treasury Board of Canada Secretariat, Directive on Automated Decision Making: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

kk) Treasury Board of Canada Secretariat, Directive on Security Management: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C

ll) Treasury Board of Canada Secretariat, Directive on the Management of Projects and Programmes (effective April 2019): https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32594

mm) Treasury Board of Canada Secretariat, Levels of security: https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html

nn) Treasury Board of Canada Secretariat, Secure Cloud Enablement and Defence https://wiki.gccollab.ca/GC_Cloud_Infocentre

oo) Treasury Board of Canada Secretariat, Standard on Metadata: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18909

pp) Treasury Board of Canada Secretariat, Standard on Security Screening: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=2811532

qq) Treasury Board of Canada Secretariat, Standard on Web Accessibility: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

rr) WCAG 2.0 A Accessibility Standards: https://www.w3.org/TR/WCAG20 and https://www.w3.org/WAI/standards-guidelines/

Appendix A – Capability and Usability Assessment (CUA)

A.1 Purpose

a) This document outlines the Capability, Usability, Accessibility and Innovation Assessment process.

A.2 Instructions

a) The Contractor must develop and submit a cloud-based Prototype Solution for Canada's assessment.

b) The Contractor must provide both support for, and unrestricted access to, the Prototype Solution, including all Prototype Solution usage rights grants, software documentation, warranty, hosting, storage, and Maintenance and Support (excluding training), waivers, non-disclosure agreements, CUA scenario test scripts and other releases to Canada for purposes of conducting the CUA assessment.

c) Access by Canada to the CUA and licensed access for one-hundred (100) Users to test the Prototype Solution is required to conduct the CUA.

d) The Contractor must provide any instructions necessary to allow Canada to use the Prototype Solution to perform the CUA Assessment.

e) Canada will provide the Contractor with sample data inputs that must be used to validate the Prototype use cases.

A.3 Selection of Contractor's Prototype Solution

a) The CUA Prototype Solution deliverables provided under the Contract will be assessed by Canada against the criteria detailed in this Appendix A - Capability and Usability Assessment to Annex A – Statement of Work.

b) The CUA will comprise four (4) individual assessment categories. These categories are as follows:

i) Part One: Capability Scenarios Assessment: Measures the functional ability of the Prototype Solution to perform and meet the specified requirements under Annex A – Statement of Work.

ii) Part Two: System Usability Scale Assessment: Measures User ease-of-use within the Prototype Solution, including overall User experience and satisfaction with the Prototype Solution.

iii) Part Three: Accessibility Usability Scale Assessment: Measures Prototype Solution User ease-of-use through the utilization of individual assistive technologies for accessibility and accommodation needs in compliance with Government of Canada Standard on Web Accessibility[1], including assessing overall User experience and satisfaction with the Prototype Solution.

iv) Part Four: Innovation Assessment: Measures innovation demonstrated by the Contractor.

c) The maximum amount of points that can be assessed is listed in the table below:

Table A-1: CUA Scoring Summary

CUA Assessment Category	Maximum Score
Part One: Capability Scenarios Assessment	700
Part Two: System Usability Scale Assessment	85
Part Three: Accessibility Usability Scale Assessment	50
Part Four: Innovation	140
Total Points	**975**

d) The sum of the scores for each individual assessment category will be calculated in accordance with the assessment criteria and maximum points listed in each category of this Appendix A. The Overall Assessment Score for the Prototype Solution will be determined by adding each of the CUA Assessment Score from all four respective CUA Assessment Categories.

e) If required, Canada will conduct at its sole discretion the Prototype on Platform (POP) test; a test of the Prototype Solution proposed by the top-ranked Contractor (identified after the CUA assessment) to confirm that it will function as described per the Contractor's Solution Cloud Service Delivery Model. Canada will document the results of the POP Test. If Canada determines that the proposed solution does not meet any mandatory requirement of the POP Test, the Contractor will be considered to have failed the POP Test and given no further consideration. With the top-ranked Contractor having failed the POP Test, Canada may, at its discretion, consider the second-ranked Contractor (identified after the CUA assessment) to conduct a POP Test of their proposed solution.

[1] For more information on the Government of Canada Standard on Web Accessibility see https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

f) With the Contractor having completed all the assessments successfully, Canada will, at its sole discretion, exercise its irrevocable option to select the Contractor to perform all or a portion of Phase 2 Work under Phase 2 – Full Solution of Annex A – Statement of Work. Canada may also, at its discretion, exercise its irrevocable option with other Contractors who participated in the CUA for all or a portion of the Work if it is determined that this would best meet the needs of Canada.

Table A-2: Capability Assessment – Scenario Scoring Legend

CAPABILITY AND USABILITY ASSESSMENT – PART ONE: CAPABILITY SCENARIOS ASSESSMENT		
Result	**Scoring**	**Description**
Not Demonstrated	0 Points	The Prototype Solution has demonstrated 30% or less required functionality related to the Capability.
Partially Demonstrated	3 Points	The Prototype Solution has demonstrated more than 30%, but less that 60% of required functionality related to the Capability.
Mostly Demonstrated	6 Points	The Prototype Solution has demonstrated 60% or more, but less than 90% of the required functionality related to the Capability.
Fully Demonstrated	10 Points	The Prototype Solution has demonstrated 90% or more of the required functionality related to the Capability.

Table A-3: CUA Scenario #1 – Partner Service Request

SCENARIO #1 – Partner Service Request **Scenario themes:** Identity Management, Case Management, CRM Directory, Query, Notification, Secure information transfer, Police and Partner Portal
User Story: A Cyber Activity Report (CAR) is received from a New Partner through secure email. The CAR provides a list of routers and IPs in Canada that have been potentially compromised by threat actors for the purposes of crypto jacking and obtaining unauthorized access to a network. Input: The CAR is received by the NC3 Unit via secured email. The NC3 Unit will enrich the request and determine any correlations with existing NC3 information and external sources. All IP addresses and router detailed information is in an excel attachment (e.g. csv) sent with the email (Indicators of Compromise (IOC) entities = 1,000). Before the receipt of this CAR, another Partner has created a "Watch List" using the P3 that contains some of the entities (e.g. IP of interest) contained in the CAR.
The Prototype Solution should enable the NC3 Unit to:
• Receive automatic email notifications that a new service request was received by email. • Securely login into the Solution. • Access a User specific work queue to view request that is automatically ingested and stored. • View the structured and unstructured data that has been automatically correlated against internal and external data. • Modify and validate the information received in the request and query results found. • Assign the request to other member(s) within the Unit or request enrichment from non-NC3 Units. • Determine and produce the information package to send back to requestor via secure email. • Add the requestor to the Partner Directory. • Close the request.
The Prototype Solution should enable a Partner to:
• Securely login to the P3. • Create a Watch List.

- Receive automatic email notification when a correlation to Watch List content is found.
- Receive secure results in the form of a report from the NC3 Unit.

Scenario #1– Scoring Grid

Indicator #		Indicators	Not Demonstrated (0)	Partially Demonstrated (3)	Mostly Demonstrated (6)	Fully Demonstrated (10)
The Prototype Solution should provide the functionality to:						
Capability	**1**	Automatically ingest a secured email, parse and validate the email contents and any indicators of compromise and allow the user to add the new partner.	☐	☐	☐	☐
	2	Automatically ingest the Excel attachment, parse, tag and validate any indicators of compromise.	☐	☐	☐	☐
	3	Automatically hash the email and attachment and store the hash.	☐	☐	☐	☐
	4	Automatically query structured and unstructured internal and external sources (e.g. MISP) and correlate data	☐	☐	☐	☐
	5	Link this Service Request with previous request(s) within the Solution.	☐	☐	☐	☐
	6	Allow an NC3 User to securely login to view the Ticket and linkages.	☐	☐	☐	☐
	7	Assign a retention period and handling protocols (e.g., TLP) for this information.	☐	☐	☐	☐
	8	Automatically send a secure email to a Partner who has a "Watch List" on these IOCs and allow them to view "Watch List" hit details within their P3.	☐	☐	☐	☐
	9	Allow an NC3 User to view, review and modify the contents of the request.	☐	☐	☐	☐

	10	Allow an NC3 User to import contact information into the Partner Directory.	☐	☐	☐	☐
	11	Allow an NC3 User to assign this request to another User for further analysis.	☐	☐	☐	☐
	12	Allow 2nd NC3 User to view this request in their work queue.	☐	☐	☐	☐
	13	Allow an NC3 User to choose what data to package together to create a report.	☐	☐	☐	☐
	14	Allow an NC3 User to hash, encrypt, and share the report through email to the originator of the request.	☐	☐	☐	☐
	15	Allow an authorized NC3 User to close the service request	☐	☐	☐	☐
Scenario #1 Score:			**/ 150**			

Table A-4: CUA Scenario #2 – Municipal Ransomware - Coordinate and Assist

SCENARIO #2 – Municipal Ransomware - Coordinate and Assist **Scenario Themes:** Identity Management, Case Management, Police and Partner Portal, Notifications, Data Analytics, Maintain Business Rules and Watch Lists, Automated Enrichment, Information Management, Online Text Chat and Document Publishing and Productivity Applications, Integration.
User Story: On March 21, 2020, a ransomware compromise impacted the Springson Ministry of Transportation (SMTO) information technology (IT) infrastructure. The SMTO contacts their Police of Jurisdiction. Systems impacted totaled approximately 3000, with 400 servers and all SMTO databases and applications affected. These systems processed approximately $50M in transactions monthly. The Police of Jurisdiction reports the incident to the NC3 using the P3 and subsequently shares indicators of compromise. Based on the severity of the incident, the Solution sets a High Severity and High Priority for the NC3 Unit. The NC3 Unit initiates a Live group Chat and a Project to facilitate, coordinate and share information with Police partners. The initial efforts begin with NC3 to Partner information sharing efforts but are quickly expanded to include other groups who may have a role in relation to this attack and investigation. A request for information is broadcast to partners via the P3. After the Broadcast to partners, two additional partners return intelligence via the P3 back to the NC3 on the same ransomware including how it has affected their jurisdiction. This includes a report (PDF) with information containing a potential foreign actor associated to this Ransomware and a suspected email address.
The Prototype Solution should enable the NC3 Unit to:
• Receive a request via the Police and Partner Portal. • Triage, Parse, Correlate and Assess the Cybercrime request. • Use Prioritization Business Rules to notify the Operational Coordination Section based on attributes of the request. • Inform Partners of the incident (Federal Cyber Law Enforcement Team, Provincial Cyber Law Enforcement team, International Joint Cybercrime Action Task Force, and a Canadian Non-Law Enforcement Partner). • Live-chat with all implicated Partners – make all implicated parties aware of incident and status, discuss next steps, how NC3 can facilitate and assist. • Create and manage a Project. • Transmit a request for information to select Partners – ask whether Partners have any information related to the Ransomware.

- Assign the request for development of Intelligence by NC3 to support POJ.
- Send Intelligence Package to Partners.

The Prototype Solution should enable a Partner to:

- Securely login to the P3
- Create and submit a request and share IOCs using the P3.
- Participate in a Live group Chat via the P3 with the NC3 and other P3 Partners.
- Receive an email notification for a request for information.
- Access the Request for Information within the P3.
- Respond to the Request for Information.

Scenario #2 – Scoring Grid

Indicator #		Indicators	Not Demonstrated (0)	Partially Demonstrated (3)	Mostly Demonstrated (6)	Fully Demonstrated (10)
Capabilities	1	Allow a P3 User to submit a Cybercrime incident and request for assistance.	☐	☐	☐	☐
	2	Automatically Triage, Parse, and Correlate the Cybercrime information including Indicators of Compromise.	☐	☐	☐	☐
	3	Determine and display Severity and Priority using the Severity Matrix and Priority Rules.	☐	☐	☐	☐
	4	Send the Operational Coordination group the request in their work queue.	☐	☐	☐	☐
	5	Allow an NC3 User to Set-up Live Chat with implicated partners and invite Police partners to join.	☐	☐	☐	☐
	6	Allow implicated P3 Agencies to participate in the live chat.	☐	☐	☐	☐

	7	Allow an NC3 User to create a Project and Task the Intelligence Group within the NC3 Unit to develop an Intelligence Package.	☐	☐	☐	☐
	8	Allow an NC3 User to send a request for information, via the P3, to select Partners – asking whether Partners have any information related to the Ransomware.	☐	☐	☐	☐
	9	Allow a P3 User to see the notification email and open the P3 to see the details of the request for information on the Ransomware incident.	☐	☐	☐	☐
	10	Allow P3 partners to reply using the P3 with either additional Intelligence that is vetted by the NC3 and added to the Project, or indication that they have no information to add.	☐	☐	☐	☐
	11	Allow an NC3 User to create and send an Intel Package containing all details related to the Ransomware to all implicated Partners.	☐	☐	☐	☐
	12	Allow an NC3 User to close the service request	☐	☐	☐	☐
Scenario #2 Score:			**/ 120**			

Table A-5: CUA Scenario #3 – Partner Requests Digital Advice and Guidance

SCENARIO #3 – Partner Requests Digital Advice and Guidance **Scenario themes:** Identity Management, Case Management, Parsing, CRM Directory, Query, Notification, Tools (Optical Character Recognition, Audio to Text, Translation), Secure Information Transfer, Integration
User Story: A request for digital advice and guidance is received from a Partner via the Police and Partner Portal. The request includes: • An image file containing an email exchange in what is believed to be in Russian language, and • An English audio file (1-2 minutes) of a conversation, with a nexus to cybercrime, between multiple individuals. As this partner does not have access to advanced digital services, they use the P3 to send a request for assistance to the NC3 Unit to translate the email exchange to the English language and provide any related information pertaining to the contents of the incoming files or conversation.
The Prototype Solution should enable the NC3 Unit to:
• Receive a request via the Police and Partner Portal. • Triage, Parse, Correlate and Assess the request. • Use Workflow Business Rules to notify the Technical Advice and Guidance Section based on the attributes of the Cybercrime request. • Allow the NC3 User to review the request. • Allow the NC3 User to access translation, audio to text conversion, and OCR services. • Allow the NC3 User to package the results. • Upon request from the Police partner, send them a disclosure package for court purposes outlining the actions the system and NC3 personnel took in relation to the original request from the POJ (including submitted and enriched data files). • Close the request.
The Prototype Solution should enable a Police Partner to:
• Securely login to the P3

- Create and submit a request using the P3 including attaching audio and images.
- Receive an email notification that indicates the information package is available on the P3 and access the information package prepared by the Technical Advice and Guidance Section.
- Receive secure results in the form of an information (disclosure) package from the NC3 Unit.

Scenario #3– Scoring Grid

Indicator #		Indicators	Not Demonstrated (0)	Partially Demonstrated (3)	Mostly Demonstrated (6)	Fully Demonstrated (10)
Capabilities	1	Allow a P3 User to submit a Cybercrime request for assistance.	☐	☐	☐	☐
	2	Automatically Triage the Cybercrime request.	☐	☐	☐	☐
	3	Determine by using Workflow Business Rules that this is a request for digital advice and guidance.	☐	☐	☐	☐
	4	Based on Business Rules, automatically assign the Ticket to the NC3 Technical Advice and Guidance Section for processing.	☐	☐	☐	☐
	5	Allow the NC3 User to view the request.	☐	☐	☐	☐
	6	Allow the NC3 User to review image file to text conversion and edit as necessary.	☐	☐	☐	☐
	7	Allow the NC3 User to translate the resulting text to English.	☐	☐	☐	☐
	8	Allow the NC3 User to convert the audio file to text.	☐	☐	☐	☐
	9	Automatically Parse and Correlate the Cybercrime information including Indicators of Compromise.	☐	☐	☐	☐

	10	Allow the NC3 User to view the following results of the processing: • The language(s) that the image and audio files contained, • The original image file, • The extracted text from the image file in the original language, • The translations of the extracted texts in English, and • The extracted text from the audio file, including distinguishing different speakers in the audio sample (Speaker diarization).	☐	☐	☐	☐
	11	Allow the NC3 User to listen to the original audio file.	☐	☐	☐	☐
	12	Allow the NC3 User to prepare a response in the form of a disclosure package including any enrichment, correlations, analysis, and findings.	☐	☐	☐	☐
	13	Allow an NC3 User to make the information available to the partner via the P3.	☐	☐	☐	☐
	14	Allow the NC3 User to notify the Police Partner via a secure e-mail that their information package is ready.	☐	☐	☐	☐
	15	Allow a P3 User to access the Information package within the P3.	☐	☐	☐	☐
	16	Allow a NC3 User to close the request	☐	☐	☐	☐
Scenario #3 Score:			**/ 160**			

Table A-6: CUA Scenario #4 – Analytics

SCENARIO #4– Analytics **Scenario themes:** Identity Management, Case Management, Query, Dashboard, Configuration, Directory, Notifications, Data Analytics, Enrichment, Secure Information Transfer, Integration with Document Publishing and Productivity Applications
User Story: Linking Scenario #2 and #3 - Analytics The NC3 Unit processed the Ransomware incident described in scenario #2 and after data from scenario #3 was translated, there is a correlation to other sources of information including a "Watch List / Be on the Look Out For" flag previously entered on the system by two other Canadian Police Services. An NC3 User queries the Solution which then searches multiple sources concurrently and displays all results. These searches include “fuzzy” searching in diverse internal and external sources, finding hits on various types of information that links these 2 incidents with other information. Queries are performed by both the NC3 Unit and the Partner. The NC3 receives a SILENT HIT as some of the data was previously flagged for Silent Hit notification. Hits include matches on IP address, email, moniker, names, and bitcoin address. The results of analysis can be formatted in a variety of User-configurable ways, including but not limited to link and other network diagrams, dashboards, maps, and customizable dashboards. Analytics is accessed by both the NC3 Unit and the Partner. Several areas of the NC3 (Operations Coordination, Intelligence Section, Digital Advice and Guidance continue, or take on new tasks/work based on this analysis managed through the case management system (tasking and workflow).
The Prototype Solution should enable the NC3 Unit to:
• Securely login into the Solution. • View that there was a SILENT HIT on some of the data. • Review and Validate the information found via correlations and query results found. • Assign the File to other member(s) within the Unit (show parallel tasking) or request enrichment from non-NC3 Units. • Query internal and external data sources simultaneously. • Access and configure the results in a variety of formats using Analytics. • Access Case Management tasking and workflow.
The Prototype Solution should enable a Police Partner to:

- Receive an email notification that indicates an information package is available on the P3 and access the information package prepared by the Intelligence Section.
- Securely login to the P3.
- Receive secure results in the form of an information package from the NC3 Unit.
- Query the data identified in the analysis.
- Access and configure the results in a variety of formats using Analytics.
- Receive a SILENT HIT.

Scenario #4 – Scoring Grid

Indicator #		Indicators	Not Demonstrated (0)	Partially Demonstrated (3)	Mostly Demonstrated (6)	Fully Demonstrated (10)
Capabilities	1	Allow the NC3 User to Login into the Solution.	☐	☐	☐	☐
	2	Allow the NC3 User to view a SILENT HIT notification.	☐	☐	☐	☐
	3	Allow the NC3 User to view the correlated query results.	☐	☐	☐	☐
	4	Allow the NC3 User to send a new request to another NC3 User.	☐	☐	☐	☐
	5	Allow 2nd NC3 User to "fuzzy" search internal sources and external sources simultaneously.	☐	☐	☐	☐
	6	The "fuzzy" search matches on IP Address, email, moniker names, and bitcoin.	☐	☐	☐	☐
	7	Allow the User to view the data including: • link and other network diagrams, • dashboards, • maps,	☐	☐	☐	☐

		• customizable dashboard, and • other.				
	8	Allow the NC3 User to prepare a response in the form of an information package including any enrichment, correlations, analysis, and findings including data visualizations.	☐	☐	☐	☐
	9	Allow the NC3 User to notify all implicated agencies via a secure e-mail notification that a new Information package is ready in the Police and Partner Portal.	☐	☐	☐	☐
	10	Allow a P3 User to access the Information package within the P3.	☐	☐	☐	☐
	11	Allow the P3 User to search the criteria identified in the Information package.	☐	☐	☐	☐
	12	Allow the P3 User to access Analytic tools in various formats.	☐	☐	☐	☐
Scenario #4 Score:			**/ 120**			

Table A-7: CUA Scenario #5 – Public Report Integration

SCENARIO #5 – Public Report Integration **Scenario Themes:** Identity Management, Public Reporting Interface Integration, Police Partner Portal, Public Complaint Severity Matrix, Case Management
The Public Reporting site will generate Complaint Files that are reported by the public or businesses. Complaint Files are ingested into the NCS automatically via a data feed from the Public Reporting Website. User Story: The NC3 Unit has received five (5) public reports from the Public Reporting site, all five for the same jurisdiction. The Police of Jurisdiction has identified that for public reports, they would like to be forwarded reports that are of high priority. They have identified that reports over a loss of $10,000 is of high priority. 1) Report A: contains data that is on an NC3 Intelligence "Indicators of Compromise Watch List". 2) Report B: reports data on a crime not within the mandate of the NC3. 3) Report C: reports a ransomware of $200 stolen. 4) Report D: reports a ransomware of $100,000 stolen. 5) Report E: reports a Software Update/Repair Scam. Victim has paid $250. Reports A, C, D and E will be ingested into the NCS. Report B will be handled by Exception. The Intelligence Section, Intake and Triage Section, the Police of Jurisdiction will all access these requests and manage these requests within the Case Management of the NCS. Report D correlates to an investigation by an international partner that wants to work with various partners (including Canadian Police) to investigate this specific type of ransomware. The Solution will highlight this correlation to an NC3 analyst and allow the analyst to add this valuable information to create an enriched report that would be sent to the POJ partner. Report E correlates to many existing Reports. The Solution will take this extensive correlation into account (e.g. extent of harm, total dollar value loss) when setting severity and highlight the correlations to an NC3 analyst.
The Prototype Solution should automatically:
• Receive requests via the Public Reporting site. • Ingest the public reports. • Triage, Parse Correlate and Assess the requests. • Identify the POJ based on location.

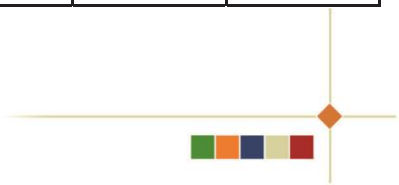
The Prototype Solution should enable the NC3 Unit to:
• Securely login into the Solution. • Assess the Public Reports. • Use “Watch List” rules to notify the Intelligence Section based on attributes of the request. • Use Exception rules to notify the Unit that data not within their mandate was captured. • Handle the Exception - forward non-mandated reports to the appropriate agency. • Use Public Complaint Severity score to identify high vs low priority public reports for the POJ. • Notify the NC3 Public reporting analyst of the requirement to enrich the high priority report before it goes to the POJ. • Send and create notifications to Police of Jurisdiction. • Others
The Prototype Solution should enable a Police Partner to:
• Receive an email notification that indicates public reports are available on the P3. • Securely login to the P3. • Configure their Public Complaint Severity Filter Rules. • Access a dashboard containing a view of Public Complaint Files that is based on the P3 Partners configurable viewing thresholds. • Select a Public Report to view details and possibly action. • Allow the P3 User to download the public complaint file. • Allow the P3 User to indicate to the NC3 that they cannot proceed with a referral. • Allow the P3 User to indicate to the NC3 that they are taking action on a public complaint file.

Scenario #5– Scoring Grid						
Indicator #		Indicators	Not Demonstrated (0)	Partially Demonstrated (3)	Mostly Demonstrated (6)	Fully Demonstrated (10)
Capabilities	1	Automatically ingest the public reports.	☐	☐	☐	☐
	2	Automatically Set Severity, Triage, Parse, and Correlate the public reports including Indicators of Compromise.	☐	☐	☐	☐
	3	Automatically correlate a request to an Intelligence Watch List and notify the intelligence group.	☐	☐	☐	☐
	4	Automatically assign the Ticket to the NC3 Intake and Triage group for processing.	☐	☐	☐	☐
	5	Automatically determine an exception based on NC3 mandate (for the applicable Public Report) and allow the NC3 User to send a message to another section.	☐	☐	☐	☐
	6	Automatically identify the POJ based on location using the postal code provided in the Public Report.	☐	☐	☐	☐
	7	For the POJ, automatically display the Public report in P3 based on POJ complaint filters.	☐	☐	☐	☐
	8	Allow the NC3 User to securely Login.	☐	☐	☐	☐
	9	Allow the NC3 User to view correlation results from the public complaints.	☐	☐	☐	☐
	10	Allow the NC3 User to enrich the complaint file.	☐	☐	☐	☐
	11	Allow the NC3 User to append enrichment results to the complaint.	☐	☐	☐	☐
	12	Allow a P3 User to securely login.	☐	☐	☐	☐
	13	Allow a P3 User to view their dashboard and drill-down to see the public complaints in their jurisdiction.	☐	☐	☐	☐

	14	Allow a P3 User to download the public complaint.	☐	☐	☐	☐
	15	Allow a P3 User to inform the NCS of actions taken or abandonment of the public complaint.	☐	☐	☐	☐
Scenario #5 Score:			**/ 150**			

Table A-8: CUA - System Usability Scale (SUS) Assessment

CAPABILITY AND USABILITY ASSESSMENT – PART TWO: SYSTEM USABILITY SCALE (SUS) ASSESSMENT					
Instructions: For each of the following statements, mark <u>one</u> box that best describes your reactions to the National Cybercrime Solution Prototype.					
Scenario #: _____ **Date:** _____/_____/_____					
#	**Indicator**	**Strongly Disagree (1 pts)**	**Disagree (2 pts)**	**Agree (4 pts)**	**Strongly Agree (5 pts)**
1	I was able to login to the system with ease.	☐	☐	☐	☐
2	I can easily navigate through requests.	☐	☐	☐	☐
3	I can easily access and view my notifications.	☐	☐	☐	☐
4	I found the Live Chat easy to use and easy to navigate.	☐	☐	☐	☐
5	I can easily create a Project.	☐	☐	☐	☐
6	I can easily task others within the solution.	☐	☐	☐	☐
7	I can easily view Silent Hits.	☐	☐	☐	☐



8	I can easily view my queue/dashboard and drilldown with ease.	☐	☐	☐	☐
9	I can easily use the Search feature and view the results.	☐	☐	☐	☐
10	I can easily access and view an information package.	☐	☐	☐	☐
11	I would like to use this Prototype Solution frequently.	☐	☐	☐	☐
12	I thought this Prototype Solution was easy to use.	☐	☐	☐	☐
13	I can use this Prototype Solution without assistance.	☐	☐	☐	☐
14	I found the various functions in this Prototype Solution were well integrated.	☐	☐	☐	☐
15	I thought there was consistency throughout this Prototype Solution.	☐	☐	☐	☐
16	I would imagine that most people would learn to use this Prototype Solution very quickly.	☐	☐	☐	☐
17	I felt very confident using this Prototype Solution.	☐	☐	☐	☐
				TOTAL SYSTEM USABILITY SCALE ASSESSMENT SCORE:	**/ 85**

Table A-9: CUA - Accessibility Usability Scale Assessment

CAPABILITY AND USABILITY ASSESSMENT – PART THREE: ACCESSIBILITY USABILITY SCALE ASSESSMENT					
Instructions: For each of the following statements, mark <u>one</u> box that best describes your reactions to the National Cybercrime Solution Prototype. This assessment with evaluate the accessibility of the Prototype Solution by people using assistive technologies.					
Scenario #: _____ **Date:** _____/_____/_____					
#	**Indicator**	**Strongly Disagree (1 pts)**	**Disagree (2 pts)**	**Agree (4 pts)**	**Strongly Agree (5 pts)**
1	The images, buttons and graphics had alternative text and were accessible.	☐	☐	☐	☐
2	Navigating the Prototype Solution with a keyboard was easy.	☐	☐	☐	☐
3	The content was easily readable because the contrast was sufficient.	☐	☐	☐	☐
4	The content was easily readable because the font was large enough.	☐	☐	☐	☐
5	The language used was plain, clear, and simple to understand.	☐	☐	☐	☐
6	The pages were properly labeled with a title.	☐	☐	☐	☐
7	The pages were not overwhelming because the quantity of content on each page was reasonable.	☐	☐	☐	☐
8	The Prototype Solution was easy to use with my accommodation tool (if applicable).	☐	☐	☐	☐
9	This Prototype Solution was designed for me and my needs.	☐	☐	☐	☐
10	This Prototype Solution was designed for most employees' accessibility and accommodation needs and requirements.	☐	☐	☐	☐
	TOTAL ACCESSIBILITY USABILITY SCALE ASSESSMENT SCORE:				**/ 50**

Table A-10: CUA - Innovation Assessment

CAPABILITY AND USABILITY ASSESSMENT – PART FOUR: INNOVATION ASSESSMENT			
The NC3 is looking for innovative technologies that would assist it in meeting its overall mandate. The innovative technologies proposed should go beyond meeting identified requirements, or relate to as yet unidentified requirements (per the BCM) to assist the NC3 in achieving its mission.			
Criteria #		**Innovation Success Criterion**	**Scoring**
Capabilities	**1**	The Contractor should document how their Solution provides technology (technologies) or functionality beyond the identified capabilities described in the BCM that will assist the NC3 in achieving its mission. Description of the enhanced capabilities should be provided using a maximum of 2000 words. A. The Contractor should clearly describe how their currently available proposed technology or functionality goes beyond identified capabilities for one or more of the four key objectives within the NC3 mandate. a) Coordination and deconfliction b) Producing actionable intelligence c) Digital advice and guidance d) Public reporting (maximum 50 points) B. For future technology or functionality, the Contractor should provide a published roadmap (that has been provided to other customers) that clearly outlines the technology or functionality. a) Coordination and deconfliction b) Producing actionable intelligence c) Digital advice and guidance	**Maximum 100 points** (A) 0 points - Insufficient or no information was provided to permit assessment; no description on how the technology or functionality would address NC3 objectives was provided; or the described technology or functionality was already expressed in the BCM. 25 points for - One key objective addressed with a clear and concise description as well as an operational example of currently available technology or functionality, how it assists the NC3, and the need was not identified within the BCM. 50 points for - Two or more key objectives addressed with a clear and concise description as well as an operational example of currently available additional technology or functionality, how it assists the NC3, and the need was not identified within the BCM. (B) 0 points - No published roadmap was provided to permit assessment or no objective addressed within the published roadmap with clear and concise description of future technology or functionality addressed along with how that future technology or functionality will assist the NC3.

		d) Public reporting (maximum 50 points)	25 Points for - Within the published roadmap, One objective addressed with a clear and concise description of future technology or functionality, along with how that future technology or functionality will assist the NC3. 50 Points for - Within the published roadmap, Two or more key objectives addressed with a clear and concise description of another type of future technology or functionality, along with how that future technology or functionality will assist the NC3.
	2	The Contractor should clearly demonstrate within their prototype how their existing technology (technologies) or functionality described in Innovation Success Criterion #1 goes beyond identified BCM capabilities in one or more of the four key objectives within the NC3 mandate. a) Coordination and deconfliction b) Producing actionable intelligence c) Digital advice and guidance d) Public reporting	**Maximum 40 points** 0 points - The Contractor has not provided demonstration of the enhanced technology or functionality. 10 points for - Each key objective clearly demonstrated within the prototype that uses innovative technologies or functionality described in Innovation Success Criterion #1.
		TOTAL INNOVATION ASSESSMENT SCORE:	**/ 140**

Appendix B – NCS Contractor Engagement – Prototype Phase

B.1 Purpose: Contractor Engagement Sessions

a) The agile systems development approach requires more interaction with Contractors to produce better results for the National Cybercrime Coordination Unit (NC3). Canada requires Contractors to thoroughly understand the requirements, be innovative and to have users at the forefront. Canada has a requirement to hold engagement sessions with Contractors to provide feedback on the prototypes as these are being developed. These sessions would be conducted in the same manner for each Contractor to allow each Contractor the same opportunity to demonstrate and seek feedback or input to their prototype work.

b) The scope of work for the Prototype Solution involves the planning, design, development, configuration, testing, and delivery of a production quality, hosted, Cloud based, working Minimum Viable Product (MVP) solution supporting up to one-hundred (100) Users in accordance with the required technical and functional requirements described herein. The Prototype Solution must not require extensive redevelopment between completion of CUA and deployment for POP Test purposes.

c) MVP:

   i) **Description:** Contractor minimally delivers the requirements for the five (5) CUA Scenarios (i.e. Prototype Solution) as per Appendix A- Capability and Usability Assessment.

   ii) **Intent**: Allow Contractor to demonstrate he can meet all the requirements in the CUA, but also, demonstrate any additional or advanced features that their product is capable within the timeframe.

d) POP Test:

   i) **Description:** At the discretion of Canada, conduct a Prototype on Platform (POP) test of the top ranked Contractor's Solution (identified during the CUA) to validate functional and non-functional requirements per Section 2.5 - Prototype on Platform (POP) Test.

   ii) **Intent:** Ensure that the Prototype, when installed per the Contractor's Cloud Service Delivery Model, meets functional and non-functional requirements.

B.2 Concept for Contractor Engagement Sessions

a) A minimum of three (3) engagement sessions with each Contractor will be held during the Prototype phase for a total of nine (9) sessions. At Canada's discretion, additional engagement sessions may be held, on an equal basis, with each Contractor. The expectation is that each contractor will participate in the sessions throughout the prototype development process.

b) The three (3) sessions will be held in the early, mid and latter periods of the Prototype Phase. Contractors and their prototypes will not be assessed during the sessions (i.e., scores are not taken in relation to the Capability and Usability Assessment (CUA)). The objective is to provide feedback and answer questions to allow the Contractor to continue to build a better prototype to better meet NC3's needs.

c) There will be common elements and rules that will apply to all three sessions, but the objectives and composition for each of the sessions will differ slightly as described below.

B.2.1 Common to all Sessions

a) Each session will be eight (8) hours long and conducted virtually with presentation capabilities and multiple points of connectivity. If in-person sessions are possible, in person sessions may be conducted at an RCMP location located in the National Capital Region.

b) Each session will allow the Contractor to demonstrate and seek input or feedback on the following capabilities based on the use cases that have been provided in the CUA:

i) Case Management;

ii) Police and Partner Portal;

iii) Artificial Intelligence (AI), Machine Learning (ML) and Natural Language Processing (NLP); and

iv) Analytics.

c) The session may also allow for the discussion of non-functional capabilities. Canada is planning on the presence of RCMP Technical Subject Matter Experts (SMEs) at the engagement sessions in order to gain an understanding of Contractor prototypes and non-functional requirements in advance of possible POP Test.

B.2.2 Responses to Contractor

a) Contractor proprietary marked information in a question will not be shared with others during the contractor engagement process. Canada's responses (and questions) to other types of questions may be shared with other contractors by the contracting authority to ensure transparency and fairness in the process. All written responses to contractor questions would go through the Contracting Authority and for documentation on the contract file.

b) As the purpose of the engagement sessions is not to formally evaluate the prototypes, Canada will not provide a score or formally confirm if something that is demonstrated by a Contractor meets or does not meet a requirement.

c) Canada will informally provide feedback to contractors on the basis of being "ON TRACK", "NOT ON-TRACK" or "UNABLE TO PROVIDE FEEDBACK AT THIS STAGE". This feedback does not constitute a formal assessment. The formal assessment will be conducted during the CUA assessment process.

i) ON TRACK: aligned to functional capabilities described in CUA.

ii) NOT ON-TRACK: misaligned to functional capabilities described in CUA.

iii) UNABLE TO PROVIDE FEEDBACK AT THIS STAGE: not enough detail to comment.

d) Regardless of the feedback that is provided, Canada will not be held responsible for the feedback during the formal CUA assessment process (for example., Canada could indicate as feedback during the engagement sessions that a requirement is deemed "ON-TRACK", but then realise during the CUA assessment that the Contractor has not met the requirement based on a more fulsome assessment and the fact that many things could change from a demonstration to the formal assessment).

e) With respect to feedback sought on usability, look, and feel, responses will be limited to "ALIGNS WITH EXPECTATIONS", "DOES NOT ALIGN WITH EXPECTATIONS" or "UNABLE TO PROVIDE FEEDBACK AT THIS STAGE".

i) ALIGNS WITH EXPECTATIONS: user friendly.

ii) DOES NOT ALIGN WITH EXPECTATIONS: not user friendly.

iii) UNABLE TO PROVIDE FEEDBACK AT THIS STAGE: not enough detail to comment.

B.2.3 Contractor Engagement Process

a) The following procedures outline the steps and safeguards to be followed during the contractor engagement sessions that will occur during the Prototype Phase of NCS development.

i) The Contractor must provide an advanced overview of what they are planning to demonstrate in each session. The overview must be provided to the RCMP at least three (3) business days prior to the demonstration to ensure that the RCMP has the appropriate SMEs present during the session.

ii) During the demonstration, there may be occasion for the RCMP to "flag" to the Contractor that questions will be asked on a certain topic.

iii) There may be a pause within the session so that a brief discussion can be held amongst key RCMP representatives.

iv) The Q&A session will allow for interaction between the RCMP and the Contractor where either side can pose and answer questions. All questions and answers will be recorded by scribes for record keeping purposes.

v) The Contractor may refer back to, or choose to re-demonstrate, their prototype solution when responding to questions from the RCMP.

vi) Any questions from the Contractor that cannot be answered directly by the RCMP during the Q&A Session will be placed in a "parking lot" to be answered in writing within five (5) business days of the demonstration. The RCMP reserves the right to decide which questions it would like to place in the "parking lot" during the session.

vii) Any questions from the RCMP that cannot be answered directly by the Contractor will be placed in a "parking lot" to be answered in writing within five (5) business days of the demonstration. The Contractor reserves the right to decide which questions it would like to place in the "parking lot" during the session. The RCMP will only respond and release information according to the security classification of the information that the RCMP is permitted to release at this stage of the process.

viii) The Contractor will receive a written transcript of the Q&As within five (5) business days of the demonstration.

ix) Any Q&A's that are proprietary in nature, as identified by the Contractor in their response, will not be shared with the other prototype Contractors. Q&As that are not proprietary in nature, will be shared with the other prototype Contractors.

B.3 Concept for Session 1

Table B-1: Concept for Session 1

Timeframe	5 weeks after beginning of prototype process		
Objective	A required early general demonstration of work to date, less focused on usability, more on technologies being used, overall concepts, RCMP providing feedback.		
Engagement Day	Morning and Early afternoon	Contractor general demos provided. Pose questions or seek feedback, does not need to cover some specific capabilities and use cases	6 hours
	Afternoon	RCMP questions and to provide unsolicited feedback	2 hours

B.4 Concept for Session 2

Table B-2: Concept for Session 2

Timeframe	10 weeks after beginning of prototype process		
Objective	The objective for the second session is for the Contractor to provide a demonstration of up to four (4) capabilities and how they work in relation to the use cases. As a minimum, this session should include a demonstration of the Police and Partner Portal and Case Management. It is up to the Contractor to determine if they will showcase all four (4) capabilities (See B.2.1. (b)) and all scenarios. This session should include more detailed and live demonstrations and explanations of functions or requirements within each of the four (4) capabilities. Visual presentation of the second session should include multiple displays so that the reviewers can see details up close.		
Engagement Day	Morning	Contractor Demos, pose questions or seek feedback. To cover at least the capabilities for session 2.	4.5 hours
	Afternoon	Allow NC3 SMEs to focus on Case Management Capabilities and Police Partner SMEs to focus on the P3. Two additional requests for the Contractor to demonstrate aspects of this capability will be permitted during this hour.	1.5 hours
	Afternoon	RCMP to request demonstration on certain elements (includes time required for the demo itself).	1 hour
	Afternoon	RCMP questions and to provide unsolicited feedback.	1 hour

B.5 Concept for Session 3

Table B-3: Concept for Session 3

Timeframe	15 weeks after beginning of prototype process		
Objective	The objective for the third session is for the Contractor to provide a fulsome demonstration of all four (4) capabilities and how they work in relation to the use cases. This should include a demonstration of all four (4) capabilities and include an interactive portion where NC3 and Police Partner SMEs are able to operate the prototype with a Contractor representative guiding them. This element will include the SMEs using the Case Management, Police and Partner Portal, AI, ML and NLP, and Analytics. Innovative technologies (CUA Part Four) can also be showcased in this session. Demonstrations do not need to cover all material demonstrated previously. This session should focus on quite detailed and live demonstrations and explanations of functions or requirements within each of the four (4) capabilities. This session must include the ability for NC3 and Police Partner SMEs working with the prototype and operating the system with the assistance of a Contractor representative. This session will mostly be accomplished virtually.		
Engagement Day	Morning	Contractor to provide general demonstrations, pose questions or seek feedback on all four (4) capabilities. If an innovative technology (technologies) are to be demonstrated (CUA Part Four), it is to occur during this timeslot.	2 hours
	Afternoon	Allow NC3 and Police Partner SMEs to "test-drive" Police and Partner Portal. Additional requests for the Contractor to demonstrate aspects of this capability will be permitted during this hour.	1.5 hour
	Afternoon	Allow NC3 and Police Partner SMEs to "test-drive" Analytics. Additional requests for the Contractor to demonstrate aspects of this capability will be permitted during this hour.	1.5 hour
	Afternoon	Allow RCMP to request demonstration on certain elements (includes time for the demo itself).	0.75 hour

Appendix C – NCS Business Capability Model

a) The NCS Business Capability Model (NCS BCM) has been developed to describe the complete scope of services and Solution capabilities that are required to enable NC3 Business Services.

b) The NCS BCM is comprised of the following:

   i) High-level Diagram depicting the major business capabilities, supporting functional and Technical Solution Capabilities;

   ii) Functional decomposition diagrams; and

   iii) Capability Descriptions in table format.

C.1 National Cybercrime Solution Capability Model

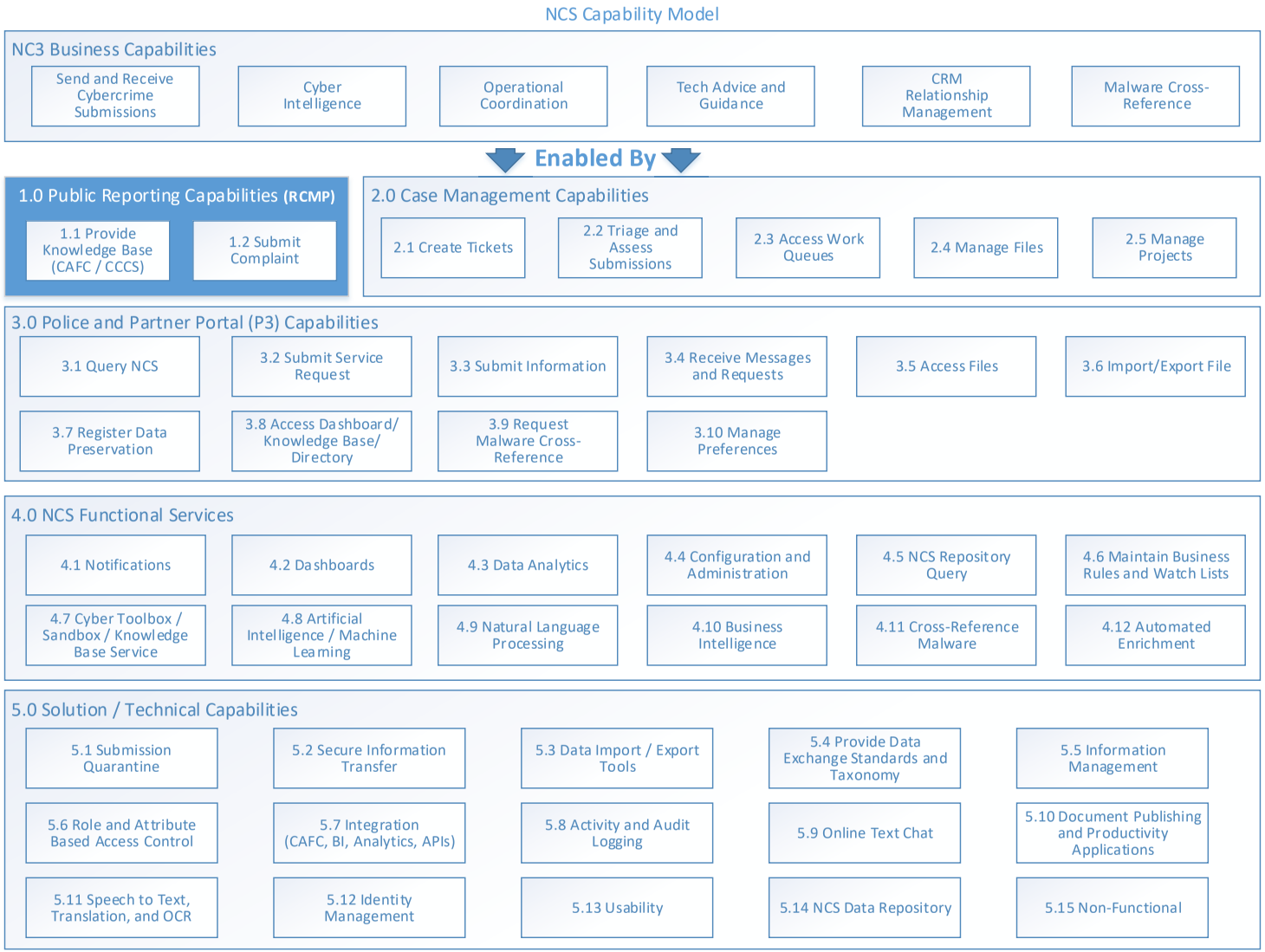

NCS Capability Model
NC3 Business Capabilities
Send and Receive Cybercrime Submissions
Cyber Intelligence
Operational Coordination
Tech Advice and Guidance
CRM Relationship Management
Malware Cross-Reference
Enabled By
1.0 Public Reporting Capabilities (RCMP)
1.1 Provide Knowledge Base (CAFC / CCCS)
1.2 Submit Complaint
2.0 Case Management Capabilities
2.1 Create Tickets
2.2 Triage and Assess Submissions
2.3 Access Work Queues
2.4 Manage Files
2.5 Manage Projects
3.0 Police and Partner Portal (P3) Capabilities
3.1 Query NCS
3.2 Submit Service Request
3.3 Submit Information
3.4 Receive Messages and Requests
3.5 Access Files
3.6 Import/Export File
3.7 Register Data Preservation
3.8 Access Dashboard/ Knowledge Base/ Directory
3.9 Request Malware Cross-Reference
3.10 Manage Preferences
4.0 NCS Functional Services
4.1 Notifications
4.2 Dashboards
4.3 Data Analytics
4.4 Configuration and Administration
4.5 NCS Repository Query
4.6 Maintain Business Rules and Watch Lists
4.7 Cyber Toolbox / Sandbox / Knowledge Base Service
4.8 Artificial Intelligence / Machine Learning
4.9 Natural Language Processing
4.10 Business Intelligence
4.11 Cross-Reference Malware
4.12 Automated Enrichment
5.0 Solution / Technical Capabilities
5.1 Submission Quarantine
5.2 Secure Information Transfer
5.3 Data Import / Export Tools
5.4 Provide Data Exchange Standards and Taxonomy
5.5 Information Management
5.6 Role and Attribute Based Access Control
5.7 Integration (CAFC, BI, Analytics, APIs)
5.8 Activity and Audit Logging
5.9 Online Text Chat
5.10 Document Publishing and Productivity Applications
5.11 Speech to Text, Translation, and OCR
5.12 Identity Management
5.13 Usability
5.14 NCS Data Repository
5.15 Non-Functional

Figure C-1: NCS– Solution and Technical Capabilities

C.2 NCS – Public Reporting Capabilities

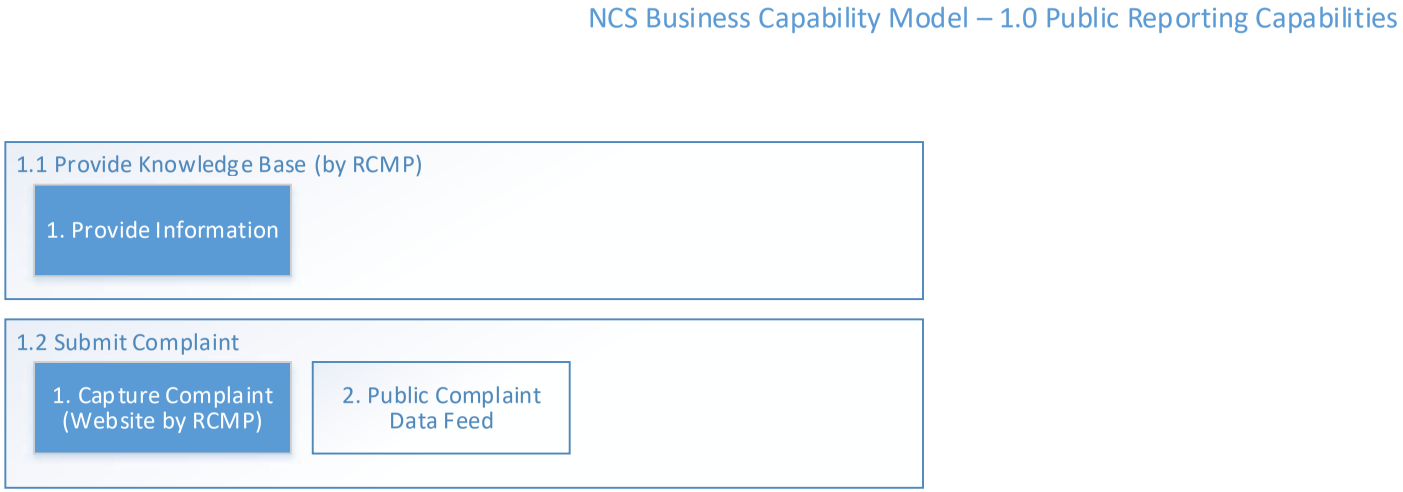


Figure C-2: NCS – Public Reporting Capabilities

Table C-1: NCS - Public Reporting Capabilities

1.2 Process Complaints The system will automatically ingest Public Reports of Cybercrimes and Frauds that have been captured via the Public Reporting Website.	
1.2.2 Public Complaint Data Feed	
1.2.2.1	The Solution must load Public Complaint Files that have been processed by the NCFRS.

C.3 NCS – Case Management Capabilities

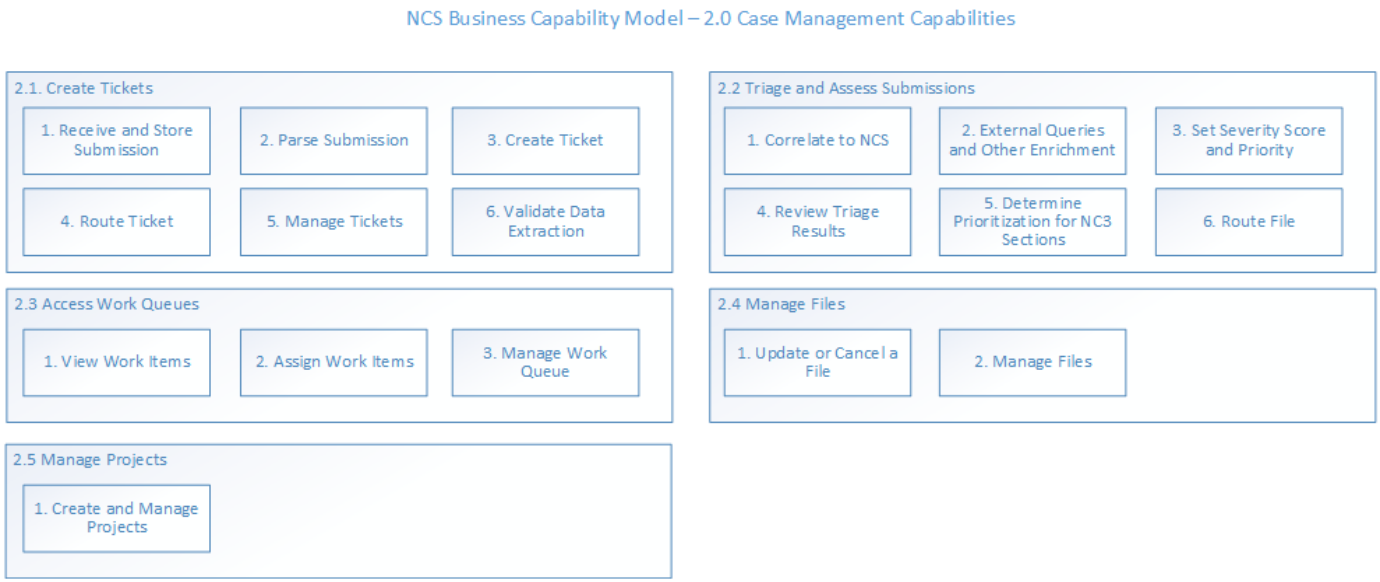


Figure C-3: NCS – Case Management Capabilities

Table C-2: NCS – Case Management Capabilities

2.1 Create Tickets The system will automatically ingest emails to create Tickets and allow Tickets to be created by Users via a User Interface. Automatic Ticket creation will parse information and populate applicable fields to create the Ticket. If applicable, Tickets will be automatically forwarded. Tickets can be forwarded manually when automatic forwarding is not applicable. The Solution will create Tickets based on P3 submissions and Public Complaint Files received via the Portal.	
2.1.1. Receive and Store Submission	
2.1.1.1	The Solution must store all submissions (including Public Report Files) and service requests, including any applicable attachments, as they are received in a read-only format.
2.1.1.2	The Solution must automatically create and store a hash of each submission, service request or attachment.
2.1.1.3	The Solution must automatically store all submission or service request metadata.
2.1.1.4	The Solution must, either through the use of tools in the RCMP cloud tenant or products supplied by the contractor, ensure that all interfaces that allow for the ingestion of data have adequate malware detection and remediation capabilities.
2.1.1.5	The Solution must automatically process submissions received via the P3. The P3 applies validations and uses templates to capture data at point of input. Therefore the NCS can use these fields in business rules and workflow rules.
2.1.1.6	The Solution must scan for exploitive material in submissions and isolate these from the file until reviewed. For example, an attachment containing an exploitive image of a child can be detected and referred for manual review by select Authorized Users.
2.1.1.7	The Solution must create a placeholder with reference number and explanation for removal, for any part of the submission that has been removed (e.g., exploitive material, malware).
2.1.2. Parse Submission	
2.1.2.1	The Solution must automatically parse submissions and service requests, including metadata as well as cybercrime Indicators of Compromise.
2.1.2.2	The Solution must classify the submission or Service Request Type to support routing and Statistical Reports. (e.g. by Crime Type, Universal Crime Reporting (UCR) Code)

Table C-2: NCS – Case Management Capabilities

2.1.2.3	The Solution must validate submissions for completeness and determine whether all required information is present in a submission or service request and fields such as dates, postal codes, cities, province are valid and formatted correctly.
2.1.2.4	The Solution must calculate any monetary values in Canadian Dollars based on the exchange rate in effect when the data was captured. Including Cryptocurrency and Fiat currencies.
2.1.2.5	The Solution must be capable of parsing information from images as well as text fields.
2.1.2.6	The Solution must perform cross-reference validation to identify submissions that contain inconsistent information in free-text fields in relation to discrete fields.
2.1.3. Create Ticket	
2.1.3.1	The Solution must be capable of creating a Ticket based on data submitted via the P3 and Public Reporting Website.
2.1.3.2	The Solution must assign a unique NC3 reference number to each Ticket.
2.1.3.3	The Solution must allow a User to create a Ticket using selectable Templates.
2.1.3.4	The Solution must automatically link all attachments, captured data and metadata to the Ticket.
2.1.3.5	The Solution must allow an NC3 User to review automatically created Tickets to confirm and approve parsing and contents and modify the Ticket to make corrections.
2.1.3.6	The Solution must validate User created Tickets to ensure all required information is present and fields such as dates, postal codes, cities, province are valid and formatted correctly.
2.1.3.7	The Solution must be capable of creating a pre-populated Ticket using a Caller's phone number received via the Call-Centre Telephony data interface.
2.1.3.8	The Solution must allow an NC3 Call Taker to complete the pre-populated Ticket based on information obtained while on the phone with a Caller.
2.1.4. Route Ticket	
2.1.4.1	The Solution must automatically route Tickets to the next step Triage and Assessment or another applicable NC3 Section using configurable business rules. (e.g. Request for Advice - to Technical Advice and Guidance, International Data Preservation Request - to 24/7 Network Team, Exception to Exception Handling User)
2.1.4.2	The Solution must be capable of automatic and manual routing of Tickets within the NC3 based on configurable workflow rules.

Table C-2: NCS – Case Management Capabilities

2.1.4.3	The Solution must be capable of routing a Ticket to a Supervisor for exception handling and review. (E.g. Threats, Out of Mandate, Other exception Rules)
2.1.5. Manage Tickets	
2.1.5.1	At a minimum, must allow Users to manage Tickets including: a. Searching b. Editing c. Cancelling d. Adding information e. Adding attachments f. Merging and Unmerging g. Splitting h. Re-Routing i. Printing
2.1.6. Validate Data Extraction	
2.1.6.1	The Solution must provide a User with the ability to review and modify a Ticket (e.g. Correct field entries from parsing and make any other edits that may be required including modifying the Classification of the Ticket).
2.1.6.2	The Solution must allow a User to manually parse and edit cybercrime IOC and observables from submissions and attachments including capturing text from image attachments.
2.1.6.3	The Solution must allow a User to populate the Partner Directory based on automatically parsed contact information.
2.2 Triage and Assess Submissions Tickets will be correlated against the NCS Data Repository and external queries will be performed to enrich the submission. Tickets that undergo enrichment are henceforth referred to as Files. After each step of enrichment, the resulting File will be triaged (scored) and assessed to determine next steps. In addition, Intelligence and Operational Coordination Section Business Rules are applied to Files to determine whether these sections should work on a File.	
2.2.1. Correlate to NCS	
2.2.1.1	The Solution must automatically correlate Ticket data to existing data in the NCS Cyber Data Repository and store the results as part of the associated Ticket.
2.2.1.2	The Solution must automatically trigger notifications to implicated parties if correlations are discovered.

Table C-2: NCS – Case Management Capabilities

2.2.1.3	The Solution must, if a new Ticket is identified as being related to an existing Ticket (e.g. it is a result of a request for more information or clarification) merge the Tickets under the original Ticket.
2.2.1.4	The Solution must provide advanced flexible correlation methods that include, but are not limited to any one or a combination of the following: a. Exact word or phrase match; b. Synonym matching; c. Fuzzy Searching (e.g. Soundex); d. Obfuscated words (e.g. pirate = p1r4t3, captain = c4pt41n, disco = d1$c0, mysite.com = mysite dot com); e. Topics; f. Tools, Techniques and Process matching; and g. Regex (Configurable)
2.2.1.5	The Solution must correlate Call-Centre Tickets to existing Public Report data (e.g. by Phone Number). If correlations exist, pre-populate the new Ticket using existing data and make previous related tickets available to a Call Taker during the call.
2.2.1.6	The Solution must be capable of cross-lingual correlating in order to identify correlations to data received or stored in multiple languages.
2.2.2. External Queries and Other Enrichment	
2.2.2.1	The Solution must allow a User to record their activities related to query and enrichment activities related to external sources such as INTELEX, SPROS, Canadian Centre for Cyber Security (CCCS), Financial Transaction and Reports Analysis Centre of Canada (FINTRAC), Open Source queries or other external data sources.
2.2.2.2	The Solution must allow the User to associate all results from external queries or enrichment activities with the File that they are enriching (e.g. make notes or attach results as PDF files, text files or images).
2.2.2.3	The Solution must allow a User to create and send a request for information to one or more P3 Partners.
2.2.3. Set Severity Score and Priority	
2.2.3.1	The Solution must use business rules to determine a severity score and priority for the File.
2.2.3.2	The Solution must utilize the contents of the File and results of each enrichment step, as well as business rules to determine a severity score for the File. The File Score and Severity may change after each result is received and processed.
2.2.3.3	The Solution must allow a User to perform further enrichment as necessary.
2.2.4. Review Triage Results	

Table C-2: NCS – Case Management Capabilities

2.2.4.1	The Solution must allow a User to review the results of Correlation and External System queries.
2.2.5. Determine Prioritization for NC3 Sections	
2.2.5.1	The Solution must identify Submissions that are of interest to sections within the NC3 e.g. Intel Section, Operational Coordination Section using a. the results of correlation to the NCS Cyber Data Repository - including hits to work in progress in a Section or hits to specific watch list contents b. other business rules
2.2.6. Route File	
2.2.6.1	The Solution must be capable of automatically notifying the Intelligence or Operational Coordination Sections of Files that have met a configurable threshold per their respective Prioritization Rules.
2.2.6.2	The Solution must allow Users to manually refer a file to another section within the NC3 in order to complete processing.
2.2.6.3	The Solution must allow the Intelligence or Operational Coordination Section to pre-emptively appropriate a File during Triage and Assessment processing.
2.2.6.4	The Solution must refer submissions that may not meet NC3 mandate to an exception handling process.
2.2.6.5	The Solution must be capable of automatically making files accessible to the associated Police of Jurisdiction.
2.3 Access Work Queues The Solution will provide configurable Work Item list functionality to provide NC3 Users with a means of managing workload. Work Queues will support assignment of work items and work item access for various Sections within the NC3. Work Queues can contain Work assignments (Tasks) related to Tickets, Files or Projects.	
2.3.1. View Work Items	
2.3.1.1	The Solution must allow a User to access work queue list(s) containing their assigned work or a pool of work from which they can draw.
2.3.1.2	The Solution must allow Users to drill down on work items to access details and other functionality required to complete the applicable task(s).
2.3.1.3	The Solution must allow a User to filter, search and sort work items in a work queue.
2.3.1.4	The Solution must allow Users to view their work items with varying levels of detail displayed. (e.g. File with Task View visible vs File summary view)

Table C-2: NCS – Case Management Capabilities

2.3.2. Assign Work Items	
2.3.2.1	The Solution must allow authorized Users to assign work items from a section level work queue pool to an individual's work queue who can then access the work via their personal work queue.
2.3.2.2	The Solution must allow Users to pull work items from a list of work items.
2.3.2.3	The Solution must allow work items to be filtered on attributes such as Crime Type or Service request type (e.g. Filter on Themes) to allow workers to focus on specific types of work items.
2.3.2.4	The Solution must be capable of configuring work queues for self-assignment or supervisor assignment.
2.3.3. Manage Work Queue	
2.3.3.1	The Solution must allow a User to re-assign a work item to another individual or return a work item to the section level pool of work items.
2.3.3.2	The Solution must allow a User to make a note on a Work Item or set a future Date to address the Work Item. A work queue notification will remind Users of future dated items.
2.3.3.3	The Solution must display a work queues columns, sort order and level of detail as they were when last viewed by the User.
2.3.3.4	The Solution must enable flexible workflow patterns - sequential, parallel, mixed workflows. For example, Files may be appropriated from Intake by Intelligence or Operational Coordination or Files may be referred for Supervisory Exception Handling based on VIP content.
2.3.3.5	The Solution must enable a User to change the state of a work item (e.g., under review, complete, rejected).
2.4 Manage Files Tickets become Files as soon as any manual enrichment activities are performed by an NC3 User or if the Severity of the Ticket is above a configurable threshold warranting a manual review. A File can be derived from one or more Tickets. Files can be updated, new links to other Files or Tickets can be created and Files can be referred to internal NC3 Sections or to external Partners for further action.	
2.4.1. Update or Cancel a File	
2.4.1.1	The Solution must allow Users to manage update or Cancel Tickets or Files. E.g. Correct information, add new information, Cancel, Park
2.4.1.2	The Solution must notify implicated parties (e.g. NC3 Sections or referred agencies) if new information is added to a File and the File is being processed or monitored by an NC3 Section.
2.4.1.3	The Solution must be able to uniquely identify a File with an identifier (ID).

Table C-2: NCS – Case Management Capabilities

2.4.1.4	The Solution must, when multiple Files are related, include the ability to indicate which File is the Master File.
2.4.1.5	The Solution must provide Users with the ability to manage Files including viewing content, printing content, making corrections, adding new information or attachments, adding Notes to File, relating to other Files, adding tasks, referring to other NC3 Sections or referring externally.
2.4.1.6	The Solution must be capable of maintaining the Status of Files.
2.4.2. Manage Files	
2.4.2.1	The Solution must provide the ability to manage all aspects of Files through a complete life cycle (e.g. Create, Assess, Edit, In-progress, Referred, Completed, Archived).
2.4.2.2	The Solution must provide the ability to refer Files to, or Files from, other sections within the NC3 or to external partners (via the P3).
2.4.2.3	The Solution must provide a User with a means of accessing and viewing past versions of File fields and attachments (e.g. if data manipulation has been applied for the purposes of analysis, or a field has been amended)
2.4.2.4	The Solution must provide the ability to manage all aspects of Data Preservation Files through their complete life-cycle including retaining relationship from Demand to Order to the Mutual Legal Assistance Treaty (MLAT) as necessary.
2.4.2.5	The Solution must allow a User to create a "disclosure" package containing all contents and activities related to a Ticket, File or Project including all Data, Metadata, Activity Logs, System Audit Logs and Attachments.
2.4.2.6	The Solution must allow a User to print any elements of the File to printer or file (e.g. PDF).
2.4.2.7	The Solution must apply configurable information security designations and respect sharing protocols according to the designated level for all outputs.
2.4.2.8	The Solution must allow an Analyst to apply configurable watermarks (e.g. “Confidential”, “Third Party Rule Applies”, “Protected B”) to all outputs.
2.4.2.9	The Solution must provide the ability for a User to find and review files at any state (based on Role Based Access Control and Attribute Based Access Control) without having them assigned to them.
2.4.2.10	The Solution must provide the ability for a User to create a hash value of any report or attachment and share the hash value with the applicable report or attachment.
2.4.2.11	The Solution must provide the ability to manage distribution lists related to a File or Project to support the delivery of reports, disclosure packages or other outputs related to the File or Project. Single or bulk issuance of Packages, Reports and Notifications

Table C-2: NCS – Case Management Capabilities

	must be supported via email or the P3. Distributions Lists must not be limited (e.g. they may include P3 Partners, Victims, other government departments, private sector organizations).
2.5 Manage Projects Create and maintain a Project to link related Files, data, implicated agencies, and outcomes. A Project will help manage related activities and tasks of implicated Users. Access to Projects can be limited to specific Users or groups. Printing and Control requirements are the same as for Files - but at the Project level.	
2.5.1. Create and Manage Projects	
2.5.1.1	The Solution must provide the ability to create and manage a Project by capturing relevant information such as, but not limited to, related File(s), Project Type, Synopsis, Date, Priority, involved Users, involved groups, involved agencies, Project Name, status, and Activities.
2.5.1.2	The Solution must assign a unique Project Number to a Project.
2.5.1.3	The Solution must provide a means of printing the contents of a Project with all features related to printing a file; as well as creating a Project level disclosure package.
2.5.1.4	The Solution must provide the ability to manage all aspects of Project through a complete life cycle (e.g. Create, Assess, Edit, In-progress, Referred, Completed, Archived).
2.5.1.5	The Solution must provide a means of assigning Users to a Project.
2.5.1.6	The Solution must provide a means of assigning a security category to a Project.

C.4 NCS – Police and Partner Portal (P3) Capabilities

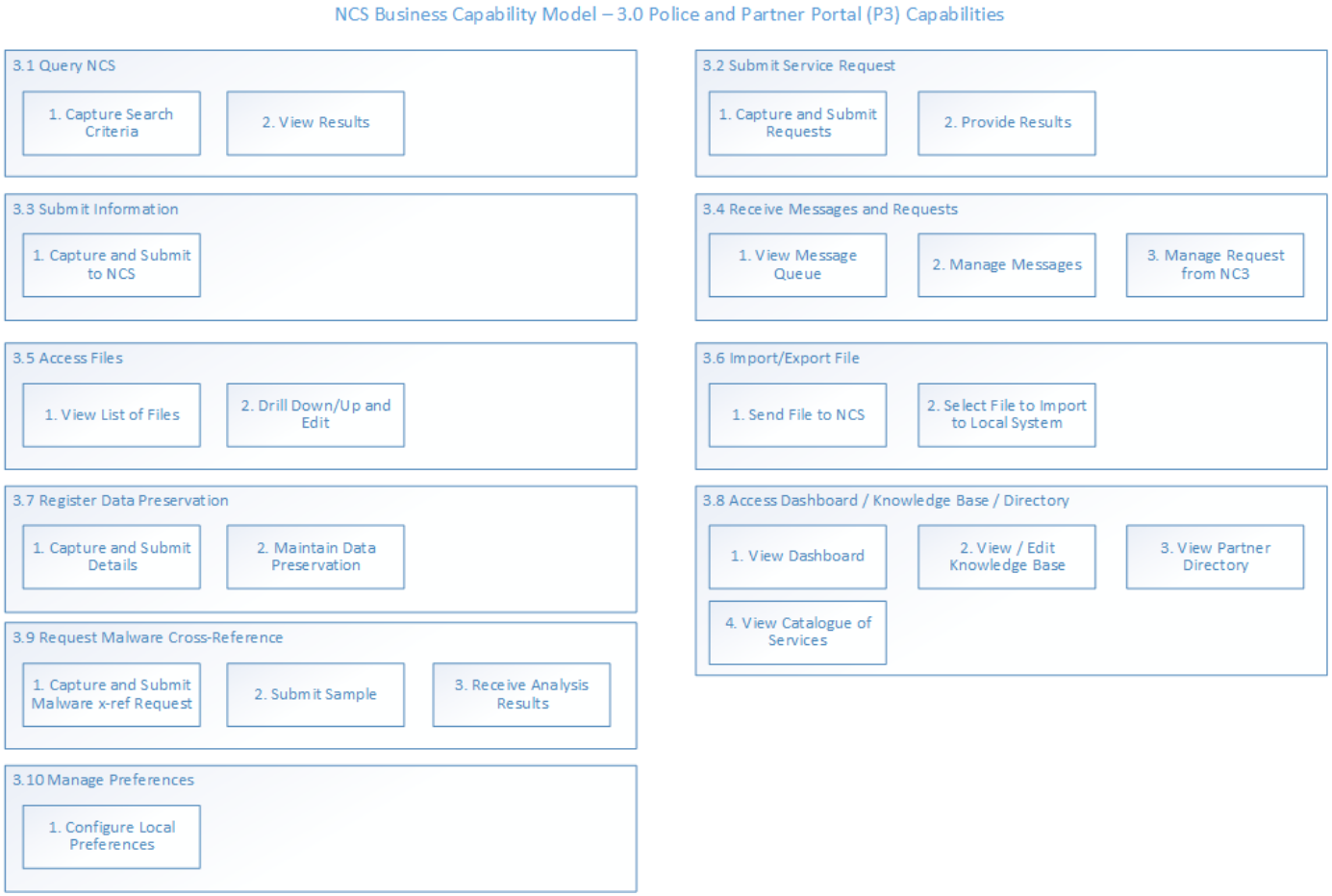


Figure C-4: NCS – P3 Capabilities

Table C-3: NCS – P3 Capabilities

3.1 Query NCS Allows a P3 Partner to query the NCS and receive a search result.	
3.1.1. Capture Search Criteria	
3.1.1.1	The Solution must provide a P3 User with the ability to enter search criteria such as but not limited to; search technique, Query Reason, IOC(s), NCS Record Types (e.g. Data Preservation, Public Complaint, LE Case Submission), Cybercrime Locations, Date limits, Target Data, Data Originator.
3.1.1.2	The Solution must validate that mandatory search fields are captured.
3.1.1.3	The Solution must be capable of advanced search techniques such as searching using exact match, proximity, wildcard, synonym, phrase matching, and account for munged and corrupted words.
3.1.1.4	The Solution must allow a User to save a Query - to be selected and re-run at some point the future.
3.1.1.5	The Solution must allow a User to create a Be On the Lookout (BOLO) or Watch list to trigger messages if queries or other activity in the NCS correlates to the BOLO or Watch list contents.
3.1.1.6	The Solution must allow a P3 User to conduct a search across all NCS data stores (e.g., Data Catalog, Object Stores, Relational Databases) with a single query.
3.1.1.7	The Solution must allow a User to conduct a search using criteria such as metadata, file contents, and file type.
3.1.2. View Results	
3.1.2.1	The Solution must display search results to the P3 User.
3.1.2.2	The Solution must include information such as; data originator, date information added to NCS, File Number, Originator Case Number, File synopsis, matching data at a minimum.
3.1.2.3	The Solution must provide a relative ranking to each search result row in order to indicate how closely the result matches the search criteria.
3.2 Submit Service Request The Solution must be capable of parsing information from images as well as text fields.	
3.2.1. Capture and Submit Request	
3.2.1.1	The Solution must allow a P3 User to create a Service Request related to services such as (list must be configurable); a. Ad Hoc search requests

Table C-3: NCS – P3 Capabilities

	b. Request to search international partners c. Access to NC3 Forensic Software Tools and Sandbox d. Request for Technical Advice and Guidance or assistance with an Investigation or Other Information e. Request for Intelligence Analysis f. Add to Partner Directory and Knowledge Base g. Request a secure P3 Chat h. Send Request to, or communicate with, another P3 Agency ("Peer-to-Peer" communications and information sharing) i. Other - generic catch all.
3.2.1.2	The Solution must facilitate the capture, validation and submission of necessary information (based on the type of request) to submit service requests to the NCS. For example, picklists of Service Request Types, and corresponding fields must be provided to assist the P3 User in completing their Service Request.
3.2.2. Provide Results	
3.2.2.1	The Solution must provide an applicable acknowledgement or results to the P3 User.
3.3 Submit Information Allows the P3 Partner to send a data submission to the NC3 for correlation with and inclusion on the NCS Data Repository.	
3.3.1. Capture and Submit to NCS	
3.3.1.1	The Solution must allow the P3 User to submit Cybercrime information to the NC3. Information may include, but is not limited to, Case Number, TLP, Security designation, Retention Date, Reason for sending, Indicators of Compromise, and Attachments.
3.3.1.2	The Solution must allow the P3 User to include an attachment(s) with their Submission or submit an attachment to add to their previous submission.
3.3.1.3	The Solution must detect if an attached File is too large and warn the User that it requires the Large File handling procedure to process.
3.3.1.4	The Solution must allow the P3 User to indicate the data sharing classification (e.g. TLP), Government of Canada security designation (e.g. Protected B) and Retention Date that is associated to the information being submitted to the NCS.
3.3.1.5	The Solution must allow a P3 User to capture a Public Cybercrime or Fraud Complaint File and submit it for processing.
3.4 Receive Messages and Requests Allows the P3 Partner to access notifications based on various scenarios and allows the NC3 to make requests to the P3 Partner. Notifications and Requests will be made available to the P3 Partners via Dashboard and Notification functionality.	

Table C-3: NCS – P3 Capabilities

3.4.1. View Message Queue	
3.4.1.1	The Solution must provide the P3 Partner with a Dashboard to view a summary of Messages or Requests from the NC3 or other P3 Agencies.
3.4.1.2	The Solution must allow the P3 User to drill down in the dashboard summary to view the applicable list of Messages and requests and related detail including Message Reason, request details and other contextual information.
3.4.2. Manage Messages	
3.4.2.1	The Solution must allow the P3 User to open the Message to view more details such as Topic, implicated agencies, other data fields, attached files, tasks or related instructions.
3.4.2.2	The Solution must allow the P3 User to maintain the status of the Messages and Requests from the NC3 (e.g. Read, Un-read, In-Progress, Actioned, Closed).
3.4.2.3	The Solution must allow the P3 User to archive messages and hide these messages from display.
3.4.3. Manage Request from NC3	
3.4.3.1	The Solution must provide the P3 User with the ability to view the details of a request from the NC3.
3.4.3.2	The Solution must facilitate creation of a response from the P3 User by providing a template that the P3 User can use to respond to the NC3 request.
3.4.3.3	The Solution must ensure that the P3 response links to the applicable File on the NCS
3.5 Access Files Will provide P3 Partners with Access to the Public Complaint Files, Tickets and NC3 referred Files (e.g. Actionable Intel package) that have been processes by the NC3. This access is provided via Dashboard Summary with a drill through to a categorized Lists.	
3.5.1. View List of Files	
3.5.1.1	The Solution must provide a categorized listing of Public Report Tickets and Files that are available to the P3 Partner.
3.5.1.2	The Solution must provide a table containing information to indicate the type of Ticket, File, Project, applicable score and severity with respect to NC3 Triage and Assessment as well as other criteria that will assist the P3 Partner in prioritizing the items.
3.5.1.3	The Solution must allow the P3 User to manage the status of the File on their queue to indicate that it has been actioned and how it has been actioned.

Table C-3: NCS – P3 Capabilities

3.5.1.4	The Solution must provide a specific categorized listing of Files that are referred to the agency based on actionable intelligence developed by the NC3.
3.5.1.5	The Solution must be capable of providing a P3 Partner with a view of Public Complaint Files that is based on the P3 Partners configurable viewing thresholds.
3.5.1.6	The Solution must be capable of limiting P3 User access to Files based on Role Based Access Control and Attribute Based Access Control.
3.5.2. Drill Down and Up and Edit	
3.5.2.1	The Solution must allow the User to view the details of any item on the queue(e.g. View File Details, View Intelligence Package) and navigate back to the queue as necessary.
3.5.2.2	The Solution must allow the P3 User to make a status update or add notes or other required attachments or data (e.g. Local RMS Case #, investigator contact information) to the Ticket, File or Project that they are accessing.
3.5.2.3	The Solution must allow the P3 User to refer a Ticket, File or Project to another Police Agency or indicate to the NC3 that they cannot proceed with a referral.
3.5.2.4	The Solution must allow the P3 User to access applicable Data Analysis functionality that is available to NC3 Users.
3.6 Import and Export File Will provide a P3 Partner with the ability to select a File from a P3 List and Import it into their local RMS. This functionality will create a file in a format that can be imported into the local RMS. Alternatively, this capability allows the P3 Partner to select a local File and Export it to the NCS. The File formats must follow a predetermined standard for data exchange between the RMS and NCS. Note that this functionality requires that the local RMS have the ability to import a structured file or create a structured file from a Case File for submission to the NCS. Note also that this interface has been described in a relatively prescribed manner. If necessary, Design and implementation details may supersede the above vision.	
3.6.1. Send File to NCS	
3.6.1.1	The Solution must allow the P3 User to select and send a formatted File (formatted per prescribed NC3 data exchange standards) to the NC3.
3.6.2. Select File to Import to Local System	
3.6.2.1	The Solution must allow a P3 User to select a File from their Work Queue of Files and indicate that they would like to import it into their local RMS.

Table C-3: NCS – P3 Capabilities

3.6.2.2	The Solution must create a File in the agreed data exchange standard and save it locally where it can be subsequently ingested by the local RMS to create a Case File. (Assumes that the RMS has the capability to ingest these files - built to an agreed upon standard)
3.7 Register Data Preservation The P3 User can enter the details of a Data Preservation Demand or Order that they are serving against a local data custodian and submit to the NCS. The NCS will correlate to the NCS Repository for deconfliction purposes.	
3.7.1. Capture and Submit Details	
3.7.1.1	The Solution must allow the P3 User to enter the details (such as; Foreign or Domestic, the subject of the Data Preservation, the data to be preserved, the data holder information, the applicable dates, the local case number and contact information) associated with a Data Preservation Demand or Order that they are serving on a Data Holder in Canada or are requesting internationally.
3.7.2. Maintain Data Preservation	
3.7.2.1	The Solution must allow a P3 User to view the Data Preservation Demands and Data Preservation Orders that they have registered.
3.7.2.2	The Solution must allow a P3 User to indicate that the Data Preservation Demand or Order is Cancelled, that the Data Preservation Order is Renewed with applicable dates or that the DataPreservation Demand or Order has led to a Production Order.
3.8 Access Dashboard, Knowledge Base, and Directory The P3 dashboard will contain a summary of referrals and other jurisdiction related information. It will provide a starting point from which the P3 User can navigate to work queues, specific requests, messages, reports and referrals as necessary.	
3.8.1. View Dashboard	
3.8.1.1	The Solution must allow a P3 User to View a Dashboard displaying summary level information and graphics with the ability to drill through to requests, messages, statistical reports, referrals or other applicable details.
3.8.1.2	The Solution must include Local Jurisdiction statistics including trends, geographic representations and Heatmaps in the P3 Dashboard.
3.8.1.3	The Solution must allow the User to customize their dashboard contents by selecting from predefined contents (e.g. "Tiles").
3.8.2. View and Edit Knowledge Base	
3.8.2.1	The Solution must allow a P3 User to browse, search, find and view a library of content and links to educational resources and job aids; frontline officer intake checklists, templates, guidelines, scenarios, tips, precedents, and case law.

Table C-3: NCS – P3 Capabilities

3.8.2.2	The Solution must allow a P3 User to Contribute material for addition to the Knowledge Base. Note that this content will first be approved for publication by the NC3.
3.8.2.3	The Solution must allow a User to download or print documents and files that are made available via the Knowledge Base.
3.8.3. View Partner Directory	
3.8.3.1	The Solution must provide P3 Users with a searchable Directory of resources (e.g., individuals and organizations) such as ISP contacts, cryptocurrency exchanges, IT Security Contacts, LE Cybercrime subject experts, cybercrime and fraud investigator contact information (NCFTA, CCCS, RCMP, FBI IC3, EC3).
3.8.4. View Catalogue of Services	
3.8.4.1	The Solution must allow a User to browse, search, find and view software tools available via the NC3 cybercrime “toolbox and sandbox”.
3.8.4.2	The Solution must allow a User to request access to Tools and schedule time in the NC3 Sandbox. Note that the "Sandbox" is scalable so access to space should not be an issue.
3.9 Request Malware Cross-Reference Allows the P3 Partner to request that the NC3 facilitate a cross-referencing or analysis of Malware. The Solution will allow the P3 User to submit a Malware Sample or Malware hash to provide for x-ref and analysis.	
3.9.1. Capture and Submit Malware x-ref Request	
3.9.1.1	The Solution must provide a P3 User with the ability to enter details regarding their Malware Cross-Reference Request (e.g. Local File #, Context, Malware Sample to Submit indicator, Intelligence Only, Related to ongoing investigation, Findings to be used in Judicial Discovery) and submit the request to the NCS.
3.9.2. Submit Sample	
3.9.2.1	The Solution must provide the P3 User with a means of submitting their malware sample.
3.9.2.2	The Solution must securely compress, hash and segregate Malware samples from other RCMP data.
3.9.3. Receive Analysis Results	
3.9.3.1	The Solution must return a message that a malware analysis is complete via the P3 dashboard.
3.9.3.2	The Solution must allow the P3 User to access the results of the Malware Analysis.

Table C-3: NCS – P3 Capabilities

3.10 Manage Preferences Allows an authorized P3 User (based on Role Based Access Control) to manage the P3 system preferences for the P3 Agency.	
3.10.1. Configure Local Preferences	
3.10.1.1	The Solution must allow an authorized P3 User to set various configuration parameters that are specific to the Agencies P3 use. Examples include; local email for alerts, Notification Options (e.g. Hourly, Daily, Weekly), and Contact Information.
3.10.1.2	The Solution must allow a P3 User to view and manage a list of Indicators of Compromise (Watch List) of specific interest to that User's organization.
3.10.1.3	The Solution must allow a P3 User to maintain Public Report threshold parameters in order to segregate actionable Public Reports from low value reports.

C.5 NCS – Functional Services Capabilities

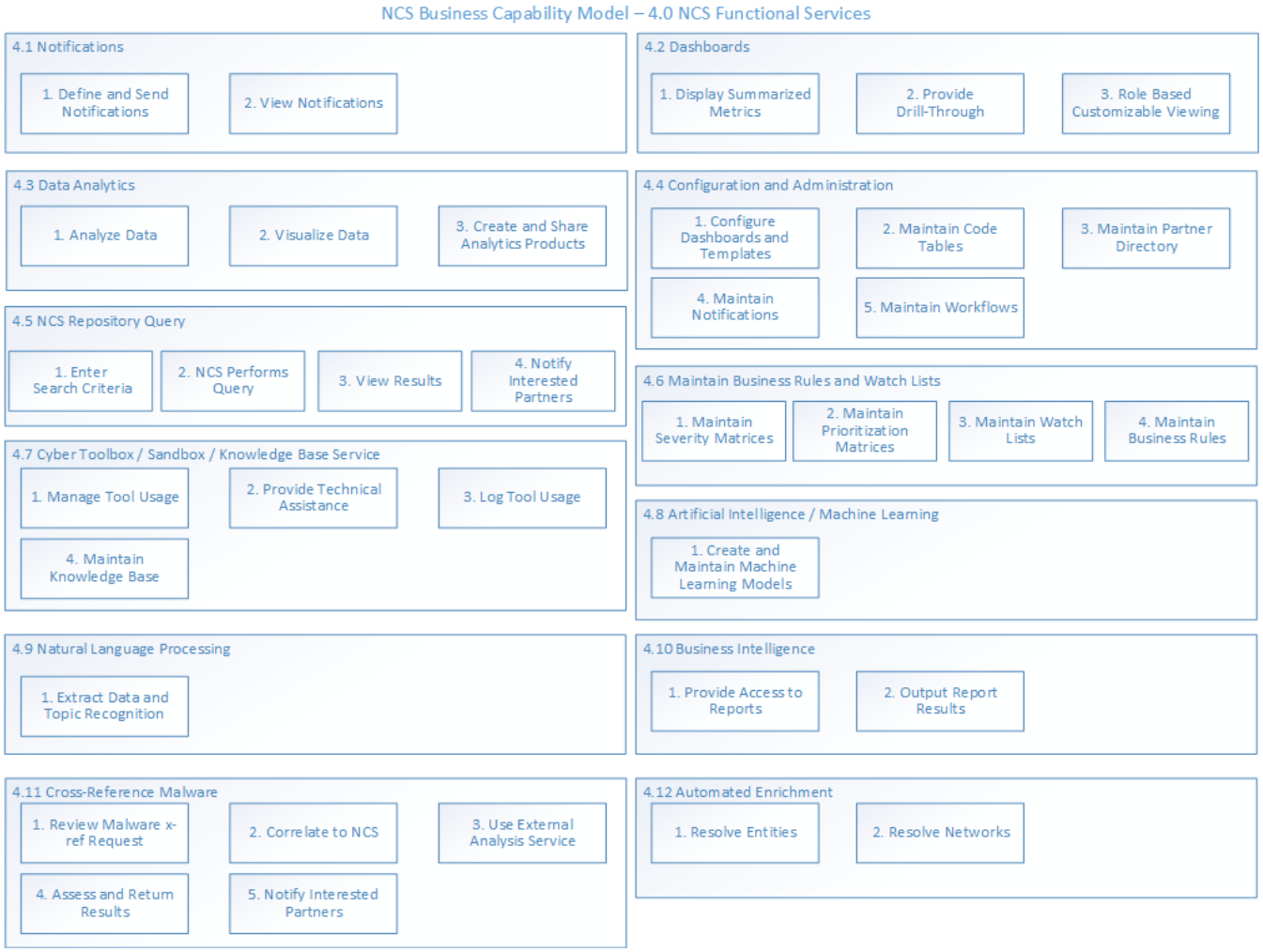


Figure C-5: NCS –Functional Services Capabilities

Table C-4: NCS - Functional Services Capabilities

4.1 Notifications Certain events within the Solution, such as data correlations, task assignments or expiry dates, will result in Notifications to implicated parties. The Solution must take into account disclosure rules to route notifications. The Solution must also display and manage notifications for implicated Users. Events that trigger Notifications are documented as capabilities in other appropriate sections of the capability model. For example, notifications are triggered based on data correlations to entities such as IOC, watch lists, search criteria history, data preservations, NC3 Intel or Operational File work in progress or related data analytics, additions of data to the repository, data preservation requests or other enrichment activities.	
4.1.1. Define and Send Notifications	
4.1.1.1	The Solution must automatically provide notifications to implicated Users, groups, LE Agencies or Cybercrime Partners based on various User or system triggers defined throughout the Solution.
4.1.1.2	The Solution must take into account all disclosure limitations including TLP and Data Security Designations when presenting notifications or data. For example, a notification, message or data display may be adjusted to include only pointer information (links) if the TLP restricts sharing or the Data Security Designation exceeds that of the recipient.
4.1.1.3	The Solution must allow an NC3 analyst to manually send a notification to a User, group, LE Agency or Cybercrime Partner. The contents of manual notifications are also subject to disclosure limitations.
4.1.1.4	The Solution must automatically log all notifications issued - no matter the means and type of notification.
4.1.1.5	The Solution must provide P3 notifications to cybercrime partners and LE agencies via email; the email will indicate that the details are available via the P3.
4.1.1.6	The Solution must notify an NC3 User if a notification cannot be delivered due to a data sharing caveat or some other business rule.
4.1.1.7	The Solution must be capable of sending notifications using email and text (defined in the notification profile) to a configurable target User or Users, in parallel with a P3 Notification. This is meant to handle off-hour notifications in certain high priority situations.
4.1.1.8	The Solution must provide Users with the ability to configure correlation business rules in order to manage the volumes of notifications.
4.1.2. View Notifications	
4.1.2.1	The Solution must allow a User to view the notifications that have been sent to them.
4.1.2.2	The Solution must allow a User to filter, sort, archive, and search for specific notifications or notification types.

Table C-4: NCS - Functional Services Capabilities

4.1.2.3	The Solution must provide the User with the ability to drill down on a notification to see the underlying File, Ticket or other entity to which the notification relates.
4.2 Dashboards Dashboards will be used to provide summary views of significant information based on the role of the user. The dashboard could provide drill through to detailed task lists and work queues that a user would use to access their daily tasks. Dashboards for managers would provide a summary of operational metrics that would provide them with real-time situational awareness of NC3 operations.	
4.2.1. Display Summarized Metrics	
4.2.1.1	The Solution must provide Dashboards containing Tiles displaying graphical views of aggregated data such as service requests, submissions and NC3 operational work in progress.
4.2.1.2	The Solution must provide NC3 Users with graphical and tabular views of current summary data containing key performance indicators for workflow activities such as: a. Intake; b. Triage; c. Assessment; d. Data Analysis; e. Intelligence Coordination; and f. Operational Coordination.
4.2.1.3	The Solution must provide authorized NC3 and P3 Users with standard graphical views containing near real-time summaries of data being ingested into the NCS Data Repository. A dashboard view may include: a. Statistical Variance Thematic Mapping; b. Fraud and Cyber Stats – regional, local, national; c. Query volumes, correlations discovered; d. Ongoing case volumes by status; and e. Trend charts.
4.2.2. Provide Drill-Through Where Applicable	
4.2.2.1	The Solution must allow a User to drill down (and up) in the Dashboard to display a list or other detailed representation of the data entities that contribute to that selected Dashboard graph or statistic.
4.2.3. Role Based Customizable Viewing	
4.2.3.1	The Solution must provide the means to allow a User to customize a standard dashboard view and save it as a User-specific Dashboard view. This includes, but is not limited to, the ability to select which tiles are to appear on their dashboard.

Table C-4: NCS - Functional Services Capabilities

4.3 Data Analytics Data Analytics capabilities will create intelligence or valuable data from raw text or images. The NC3 will ingest data from several sources that will be transformed as necessary and analysed using criminal intelligence analysis tools. The resulting intelligence will be used to guide decision making and produce actionable intelligence for law enforcement.	
4.3.1. Analyze Data	
4.3.1.1	The Solution must provide the ability to perform in-depth analysis on data in the NCS Data Repository; visualize data (e.g., raw data, cleansed data, results of code execution, results of models); and export or associate models, outputs and analytics projects for sharing with P3 Users.
4.3.1.2	The Solution must allow the User to work in an interactive and collaborative data science environment to manipulate data, code and models associated with a File and in conjunction with other data sources; temporarily store data, cleanse and transform data; build analytical models, write code, execute code, in whole or in part; version control analytics projects and associated files; associate or share files, projects and contained data and models with other Users; visualize data (e.g., raw data, cleansed data, results of code execution, results of models); and export or associate models, outputs and analytics projects for sharing with P3 Users.
4.3.1.3	The Solution must provide users with tools to automate the gathering of open source information. Open Source Intelligence (OSINT) tools should be able to facilitate the identification of entities (e.g. companies, victims or potential victims, physical addresses, potential suspects) given various criteria such as company names, physical addresses, IP Addresses and URLs.
4.3.2. Visualize Data	
4.3.2.1	The Solution must provide the means to produce and display charts and diagrams such as, but not limited to, link charts, flow charts, event charts, geospatial maps and other graphical depictions from the data enriched by the analytic tool.
4.3.2.2	The Solution must provide the means to save the Intelligence Product text, diagrams and graphical images in an exportable file format such as Adobe Acrobat PDF.
4.3.2.3	The Solution must allow a User to create comprehensive Intelligence Products containing selected text and graphical representations of the data.
4.3.2.4	The Solution must allow the Intel Analyst to apply TLP classification and redaction to intelligence packages and products or other information being disseminated.
4.3.2.5	The Solution must provide Users with the ability to view and print Analytics Reports (e.g., Intelligence Products).

Table C-4: NCS - Functional Services Capabilities

4.3.3. Create and Share Analytics Products	
4.3.3.1	The Solution must allow an analyst to create and share Analytics Reports, outputs or related information (e.g., Situational Awareness, Victim Notifications, Analysis Results; Partial or Final) with selected agencies and Users via the P3, email, or other secure portal.
4.3.3.2	The Solution must allow an Analyst to apply configurable watermarks (e.g. “Confidential”, “Third Party Rule Applies”, “Protected B”) to Analytics Reports.
4.3.3.3	The Solution must allow a User to selectively redact (block-out or withhold non-disclosable information) specific information fields or free text to protect sources or other individually identifiable persons that are not the subject of the file.
4.3.3.4	The Solution must allow a User to create and attach hash values of reports and attachments that they can distribute with the report or attachment.
4.3.3.5	The Solution must support review and approval of reports, notifications or other outputs (by authorized NC3 Users) prior to distribution.
4.3.3.6	The Solution must allow a user to share approved reports, such as Victim Notifications, directly with a victim or potential victim.
4.4 Configuration and Administration NCS Configuration and Administration capabilities include functionality necessary to manage the configuration and maintenance of the system. This capability encompasses management of (but not limited to) User Accounts, Code Tables, Dashboard Tiles, Partner Information, Public Key Management and other system parameters.	
4.4.1. Configure Dashboards and Templates	
4.4.1.1	The Solution must allow an authorized NC3 User to manage standard dashboard views or contents by creating, modifying or deleting Tiles that can be saved and referred to by Users.
4.4.2. Maintain Code Tables and Help Content	
4.4.2.1	The Solution must allow an authorized User to manage the content of data tables used for purposes of validating encoded data inputs and displaying pick lists in the user interface.
4.4.2.2	The Solution must allow an authorized NC3 User to manage on-line help content.

Table C-4: NCS - Functional Services Capabilities

4.4.3. Maintain Partner Directory	
4.4.3.1	The Solution must allow an authorized User to manage profile information related to NC3 Cybercrime Partners, Law Enforcement Agencies and all other stakeholders with which the NC3 interacts. Profiles include information such as Partner Type, Contact Information, Level of Cybercrime Expertise, and Escalation Contact and Procedure.
4.4.3.2	The Solution must allow an authorized NC3 User to manage referral preferences, thresholds and rules as well as subordinate and superior relationships between Law Enforcement agencies for the purposes of referrals.
4.4.3.3	The Solution must provide a means of associating and maintaining attributes to assist in identifying responsible Police of Jurisdiction. Attributes may include geographic location, street address, mailing address (Postal Code), IP Address.
4.4.3.4	The Solution must provide potential users with a means of submitting online applications for access to the NCS (including the P3).
4.4.3.5	The Solution must provide authorized users with the ability to review, approve and initiate on-boarding procedures related to applications for user accounts.
4.4.4. Maintain Notifications	
4.4.4.1	The Solution must allow an authorized User to create, modify or remove notification templates.
4.4.4.2	The Solution must allow an authorized User to manage the rules under which a notification must be issued and which template must be used.
4.4.4.3	The Solution must allow an authorized User to indicate, by notification template and business rule criteria, that an e-mail and a text message must also be sent to the recipient of the notification.
4.4.5. Maintain Workflows	
4.4.5.1	The Solution must allow an authorized NC3 User to create, modify or remove workflows. This includes, but is not limited to, automated task creation and automated assignment of tasks or files to Users or groups.
4.4.5.2	The Solution must allow an authorized NC3 User to manage standard Templates for P3 Users to submit structured Submissions and Service Requests.

Table C-4: NCS - Functional Services Capabilities

4.5 NCS Repository Query NCS Repository query capabilities will provide Users (NC3 and P3) with ability to query a central store of cybercrime related information using advanced techniques to account for the cybercrime specific aspects of the data. NCS queries will also be capable of triggering correlation notifications based on mutual interest discovered via query results or use of the same query parameters.	
4.5.1. Enter Search Criteria	
4.5.1.1	The Solution must provide the ability to query all or selected NCS Data Repository contents. For example, Date limits, geographic limits or crime type limits might be used as parameters.
4.5.1.2	The Solution must provide flexible search matching methods including, but not limited to: a. Exact word or phrase match; b. Proximity searches; search criteria words within a specified number of words from each other; c. Proximity searches within sentences or paragraphs; d. Wildcard searches; e. Boolean search; f. Synonyms of words specified search criteria; g. Fuzzy Searching (e.g. Soundex) h. Obfuscated words (e.g. pirate = p1r4t3, captain = c4pt41n, disco = d1$c0, mysite.com = mysite dot com); and i. Any combination of search criteria identified above within the same query.
4.5.1.3	The Solution must, for all NC3 and P3 Users, provide a natural language query interface and a forms-driven UI to guide the User in defining the criteria for a search.
4.5.1.4	The Solution must provide the User with the option of saving the search criteria for use in a future query.
4.5.1.5	The Solution must allow the User to indicate that the query must be silent. The results of a silent query are returned to the querying agency only. The Silent Query will not be used to trigger a "same query criteria" notification. Note this feature will not override notifications to NC3 Users. It will apply to notifications to external LE agencies and partners only.
4.5.1.6	The Solution must search a query history for similar searches and provide a response to indicate if others have queried the same or similar criteria in the past.
4.5.1.7	The Solution must allow a User to search on applicable fields or attributes in the NCS Repository including, but not limited to, Indicators of Compromise, Hash Values, Tools Techniques and Procedures, Ticket, File or Project Attributes including free text fields.
4.5.1.8	The Solution must by default, if more than one criteria is used, return results that match all criteria (per chosen search method) and also allow the User to override and get results that match any criteria.

Table C-4: NCS - Functional Services Capabilities

4.5.1.9	The Solution must allow a User to conduct a federated search across all NCS data stores (e.g., Legacy IOC Data, Data Catalog, Object Stores, Relational Databases) with a single query.
4.5.1.10	The Solution must, provide the User with a means of indicating a minimum score for their query - or a minimum score for an automatically performed query. Results not meeting the minimum score will not be displayed.
4.5.2. NCS Perfoms Query	
4.5.2.1	The Solution must be able to perform a query against the NCS Repository using the criteria specified by the User.
4.5.2.2	The Solution must apply Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) (e.g. TLP, Info. Security Designation) rules to the search results to determine what data can be returned to the User.
4.5.2.3	The Solution must, for data that was deemed to be not releasable, indicate in the search results that additional information is available and provide the data originator's contact information.
4.5.2.4	The Solution must generate a score for each result that is returned to the User based on the measure of similarity to the query criteria.
4.5.2.5	The Solution must make the result along with match score, type of correlation found (for example, a correlation to a previous query, data preservation, data submission, complaint file) and other summary data to be displayed to the query User.
4.5.2.6	The Solution must be capable of cross-lingual searching in order to retrieve results stored in a language different from the criteria.
4.5.3. View Results	
4.5.3.1	The Solution must provide the capability for the User to view the search results.
4.5.3.2	The Solution must provide the capability for the User to filter and sort any of the data columns presented in the result. Default orders must take into account the context of the search; factors such as applicable scoring, Dates or Alphabetic ordering may be used as default orders.
4.5.3.3	The Solution must provide the capability for the User to drill down on any selected results row to view details of the matched data. For example - open the related File, Data Preservation – and drill back up to the result.
4.5.3.4	The Solution must allow a User to print a search result or save a search result.
4.5.3.5	The Solution must apply highlighting to searched terms within applicable results and documents (configurable option).

Table C-4: NCS - Functional Services Capabilities

4.5.4. Notify Interested Parties	
4.5.4.1	The Solution must raise required notifications if it discovers a correlation to the NC3 Repository or to a similar query previously performed. If the Silent Query indicator is set, the behaviour must change to allow only notifications to the NCS to be delivered.
4.5.4.2	The Solution must support Silent Hit Functionality. If there is a correlation to existing data with a Silent Hit tag, do not include the data in the result, but notify the agency that contributed the data. Hits to query history will be returned.
4.6 Maintain Business Rules and Watch Lists Business Rules will be used to identify the severity of submissions received by the NC3. In addition, business rules will be used to identify submissions of interest to various sections of the NCS. When a submission of interest is discovered, the applicable section within the NC3 will be notified.	
4.6.1. Maintain Severity Matrices	
4.6.1.1	The Solution must allow an authorized User to define the business rules necessary to derive a severity score for every service request, submission and public complaint ingested by the Solution.
4.6.2. Maintain Prioritization Matrices	
4.6.2.1	The Solution must allow an authorized User to define business rules (Prioritization Matrices) that will identify submissions of interest to a specific section within the NC3. e.g. the Intelligence Section or the Operational Section. Sections can define their own business rules.
4.6.2.2	The Solution must allow, an authorized User to modify the rules and thresholds for each defined Prioritization Matrix.
4.6.3. Maintain Watch Lists	
4.6.3.1	The Solution must allow an NC3 User to manage watch lists of Indicators of Compromise, Tactics Techniques and Procedures (TTP) or other entities of specific interest to a section within the NC3.
4.6.3.2	The Solution must allow Watch Lists to be created for various sections of the NC3 Unit.
4.6.4. Maintain Business Rules	
4.6.4.1	The Solution must allow an authorized User to configure business rules which govern activities such as system workflows.
4.6.4.2	The Solution must allow authorized NC3 Users to set, remove or override for NC3 (temporarily or permanently) Silent Hit indicators. Note that the NC3 may be requested to apply Silent Hit indicators to data - or may need to override to them to gain situational awareness to support operational coordination.

Table C-4: NCS - Functional Services Capabilities

4.7 Cyber Toolbox, Sandbox, and Knowledge Base Service The NC3 will offer a service to Canadian Law Enforcement that will enable police agencies to use cybercrime forensic related software applications. In addition, the NC3 will provide a "sandbox" in which agencies can analyse data using these tools, while also leveraging the ability to correlate to the NCS Cyber Data Repository as well as populate the repository with results. In addition, the NC3's capabilities to maintain the Knowledge Base provided via the P3 are described here.	
4.7.1. Manage Tool Usage	
4.7.1.1	The Solution must be capable of managing requests to use cybercrime forensic applications and services that are provided by NC3.
4.7.2. Provide Technical Assistance	
4.7.2.1	The Solution must allow NC3 resources to track activities related to tool set-up and usage assistance to Law Enforcement.
4.7.3. Log Tool Usage	
4.7.3.1	The Solution must be capable of incorporating the results of forensic analysis tools into the NCS Repository for the purposes of correlation, deconfliction and situational awareness.
4.7.3.2	The Solution must be capable of notifying NC3 Users when correlations are made based on results of tool usage in the sandbox.
4.7.4. Maintain Knowledge Base	
4.7.4.1	The Solution must allow Users to manage the Knowledge Base contents made available to P3 Users and the Public Portal website.
4.7.4.2	The Solution must allow Users to maintain a catalog of NC3 services.
4.7.4.3	The Solution must allow a User to review content that has been contributed by P3 Partners, edit and make it available via the Knowledge Base.

Table C-4: NCS - Functional Services Capabilities

4.8 Artificial Intelligence and Machine Learning Machine Learning (ML) may be utilized in several processes within the NCS. As part of the Submission Triage process, ML may be used to determine the relative score of submission with respect to solvability, severity and priority. The ML algorithms may also be used to make workflow decisions such as determining the next step necessary to process a submission or service request once it has been Triaged. The goal will be to automate some of the aforementioned decision-making activities using ML to implement continuously adapting and learning automated processes.	
4.8.1. Create and Maintain Machine Learning Models	
4.8.1.1	The Solution must allow the deployment of machine learning models to the process of triaging information received by the NCS. As a part of Triage, the ML process can be used to score, set severity, set priority and suggest the next step for submissions and service requests. The ML process may use the results of NLP and data from the NCS Cyber Repository to perform this activity.
4.8.1.2	The Solution must allow the deployment of machine learning models to the NLP process to adapt to new topics, indicators and observables. The Solution must also apply machine learning to recognize variations in data element values that have the same meaning.
4.8.1.3	The Solution must support the RCMP in meeting the Government of Canada's Guiding Principles on use of AI and Directive on Automated Decision-Making[1]. The Solution will be assessed against the Algorithmic Impact Assessment[2] (AIA).
4.8.1.4	The Solution must ensure that decisions made using AI are explainable. Explainable methods are required (as opposed to "Black Box" AI) in the event that decisions are questioned during legal proceedings.
4.8.1.5	The Solution must allow machine learning models to be applied for reasons such as, but not limited to, the following: a. Identification of precursors - where events, when seen, may indicate an activity of interest will follow; b. Development of victim profiles - where different demographics may require variations in law enforcement support and response levels; c. Development of threat actor profiles - with the aim of identifying an individual who may be a threat; d. Identification of enablers and criminal infrastructure – including, but not limited to, service providers, dark web markets for software and services, and brokers; e. Development of profiles for entities (e.g.,devices, services, locations, and other "non-human" cyber actors); f. Enabling statistical simulations - including hypothesis testing and what if analysis; g. Characterizing events such as changes in signature over time;

[1] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

[2] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html

Table C-4: NCS - Functional Services Capabilities

	h. Enabling intelligence activities – including, but not limited to, development of activity flows, commodity flows, crime pattern analysis, financial analysis, and market profiles; i. Optimizing queries; j. Optical character recognition (OCR); k. Automating Input Optimization and Response; l. Conducting Sentiment and Sematic Analyses; and m. Translation and Accessibility functionalities.
4.8.1.6	The Solution must allow machine learning models to be easily coded, trained, tested, optimized (e.g., hyper-parameter optimization) and deployed to production (e.g., triage and decision management component) from within the data science environment (see 4.3.1).
4.8.1.7	The Solution must allow machine learning models to be saved, versioned, and retrieved from within the Data Science Environment as well as have versions tracked through performance metrics and measurements once deployed into production (e.g., triage and decision management component).
4.9 Natural Language Processing (NLP) NLP will be used to perform text analytics that will extract useful data and insights from unstructured text. The goal of NLP is to reduce the manually tedious burden of data parsing, analysis and searching while increasing the NC3s capacity and capabilities to derive intelligence from large raw data sources. NC3's text analytics function will be automated, faster and more accurate than a manual text analytics Solution.	
4.9.1. Extract Data and Topic Recognition	
4.9.1.1	The Solution must use NLP and Text Analytics to provide automatic named entity data extraction capabilities to extract cybercrime data such as cyber observables; indicators; incidents; targets; adversary and defensive tactics, techniques, and procedures (TTPs); campaigns; courses of action; cyber actors from unstructured data (text and images).
4.9.1.2	The Solution must use NLP to provide automatic named entity data extraction capabilities to extract submission and service request data from free text to classify the type of service request or submission. (e.g. by Crime Type)
4.9.1.3	The Solution must recognize sentiment and raise notifications based on User configured business rules. E.g. recognize self-harm, violence, threats.
4.9.1.4	The Solution must provide Users with tools to monitor and evaluate and adjust as necessary the machine learning processes.
4.9.1.5	The Solution must provide an automated speech and audio to text capability.
4.9.1.6	The Solution must include the ability to indicate non-native text in a text file.
4.9.1.7	The Solution must include the ability to identify the language(s) being spoken in an audio file.

Table C-4: NCS - Functional Services Capabilities

4.9.1.8	The Solution must include the ability to identify individual speakers in an audio file.
4.9.1.9	The Solution must automatically validate data to identify frivolous submissions or values within submissions. For example, identify Public Reports where loss is exaggerated, or the report is not cybercrime or fraud related (e.g. bicycle theft). These validation rules must be configurable. Note: This will support more accurate reporting of cybercrime and fraud losses.
4.10 Business Intelligence The system will provide information to support Business Intelligence (BI) using reports, dashboards and other means. BI is intended to provide performance metrics related to the NC3 Business, Cybercrime and Fraud Trends ranging from local to national scales, Operational workflow metrics – automated and manual functions, Situational awareness information to applicable NC3 partners, Strategic Policy review and development, and Cybercrime and Fraud Statistical Analysis (Canadian public, intelligence community).	
4.10.1. Provide Access to Reports	
4.10.1.1	The Solution must be capable of producing and sharing real-time ad hoc and customized reports.
4.10.1.2	The Solution must provide Reports including, but not limited to, the following: a. Report on cybercrime and fraud trends and statistics for both operational (e.g. number of queries via the Police and Partner Portal, number of new malware identifications), and strategic needs (e.g. annual number of referrals closed, in progress or not acted upon); b. Report metrics on submissions, assistance requests, queries processed, de-conflictions found, investigations in progress and completed, Partnerships established, and private partner engagements; c. Publish cybercrime or fraud bulletins for various audiences including Police and Partner Portal Users, or general public via the Public Reporting Website knowledge portal; d. Record stats and related metadata based on cybercrime and fraud data provided by cybercrime partners and stakeholders; e. Provide Statistics Canada - Canadian Centre for Justice Statistics (CCJS) with data on cybercrime and fraud in Canada. (Possibly develop a prescribed format for this data exchange.); and f. Provide the ability to generate graphical content for reports including, but not limited to, graphs, charts, tables and output products generated from the visualization tools (see capability 4.3.4).
4.10.2. Output Report Results	
4.10.2.1	The Solution must provide NC3 User with the ability to review the contents of the reports and publications.
4.10.2.2	The Solution must allow the NC3 User to disseminate and share reports as required.
4.10.3.3	The Solution must, based on business rules, auto-disseminate reports to designated parties (e.g. Reports to Statistics Canada).

Table C-4: NCS - Functional Services Capabilities

4.10.3.4	The Solution must allow a User to attach reports to Files.
4.10.3.5	The Solution must allow a user to export reports in a variety of formats (e.g. Excel, CSV, PDF, etc.)
4.11 Cross-Reference Malware Allows for the cross-referencing malware samples from Canadian law enforcement against a national repository of police-submitted malware reports as well as selected domestic and international malware Solutions.	
4.11.1. Review Malware x-ref Request	
4.11.1.1	The Solution must enable an NC3 User to select an individual request from a list of Malware Identification requests.
4.11.1.2	The Solution must enable an NC3 User to review the request and record any notes or observations that are required.
4.11.1.3	The Solution must enable an NC3 User to manually identify and store IOCs from the submission that were not auto extracted during intake and triage.
4.11.1.4	The Solution must enable an NC3 User to adjust the severity index and priority of the submission as set during intake and triage.
4.11.2. Correlate to NCS	
4.11.2.1	The Solution must automatically query the data repository to correlate the malware sample hash value and other IOCs with data already stored in the data repository.
4.11.2.2	The Solution must enable an NC3 User to perform additional queries against the data repository if required.
4.11.2.3	The Solution must update the submission with the results of the automated and manual queries.
4.11.2.4	The Solution must enable, In the case where no match ids found on the submitted hash value, an NC3 User to create a notification via the P3 to the originating agency with instructions on how to submit the malware sample to NC3.
4.11.2.5	The Solution must receive the malware sample in a secure "drop box" location. Note: The system must securely and safely segregate Malware samples from the RCMP Corporate IT environment.
4.11.2.6	The Solution must generate a hash value for the received file and store it in the data repository.
4.11.3. Use External Analysis Service	
4.11.3.1	The Solution must enable the NC3 User to send a request along with the submitted malware sample, while ensuring that the sample remains in an air-gapped environment, to an external malware analysis service.
4.11.3.2	The Solution must store the results of analysis in the data repository once the analysis results have been received,.

Table C-4: NCS - Functional Services Capabilities

4.11.3.3	The Solution must alert the NC3 User if a response from the malware analysis service is not received after a configurable length of time.
4.11.4. Assess and Return Results	
4.11.4.1	The Solution must enable the NC3 User to review the results of the enrichment queries and the malware analysis (if a sample was analyzed).
4.11.4.2	The Solution must enable the NC3 User to create a Malware Analysis Report including content such as malware variant, summary, findings and recommendations.
4.11.4.3	The Solution must enable the NC3 User to send the Malware Analysis Report to the requesting agency.
4.11.5. Notify Interested Parties	
4.11.5.1	The Solution must enable the NC3 User to send the Malware Analysis Report to Law Enforcement Partners.
4.11.5.2	The Solution must enable the NC3 User to create a Malware Bulletin and post the bulletin on the P3 based on the results of the analysis.
4.12 Automated Enrichment Allows for the automated resolution and enrichment of data using AI techniques including entity resolution and network analysis.	
4.12.1. Resolve Entities	
4.12.1.1	The Solution must be capable of automatically resolving entities (e.g., deconflict an on-line identity, combine "John Smith" and "J. Smith" that both live at the same address).
4.12.1.2	The Solution must allow a User to review resolved entities and separate entities that were erroneously resolved to a single entity.
4.12.1.3	The Solution must automatically correlate extracted data to data already existing in the NCS Cyber Data Repository and raise notifications for NC3 Users to review. E.g., Could be result of NLP, Correlation Query or Data Analysis
4.12.1.4	The Solution must allow a User to view and manipulate entities with a link and network visualization tool.
4.12.1.5	The Solution must provide a means of identifying Police of Jurisdiction based on File attributes and IOCs such as geographic location, street address, mailing address, IP Address. E.g. Given the addresses of implicated victims in a File, automatically identify all of the applicable POJs responsible for the victims locations - to facilitate communication, referral and coordination.
4.12.2. Resolve Networks	
4.12.2.1	The Solution must be capable of automatically identify links between resolved entities (e.g., similar identifying information).

Table C-4: NCS - Functional Services Capabilities

4.12.2.2	The Solution must allow a User to review identified links and separate entities that were erroneously resolved to be linked.
4.12.2.3	The Solution must allow a User to view and manipulate links with a link and network visualization tool.

C.6 NCS – Solution and Technical Capabilities

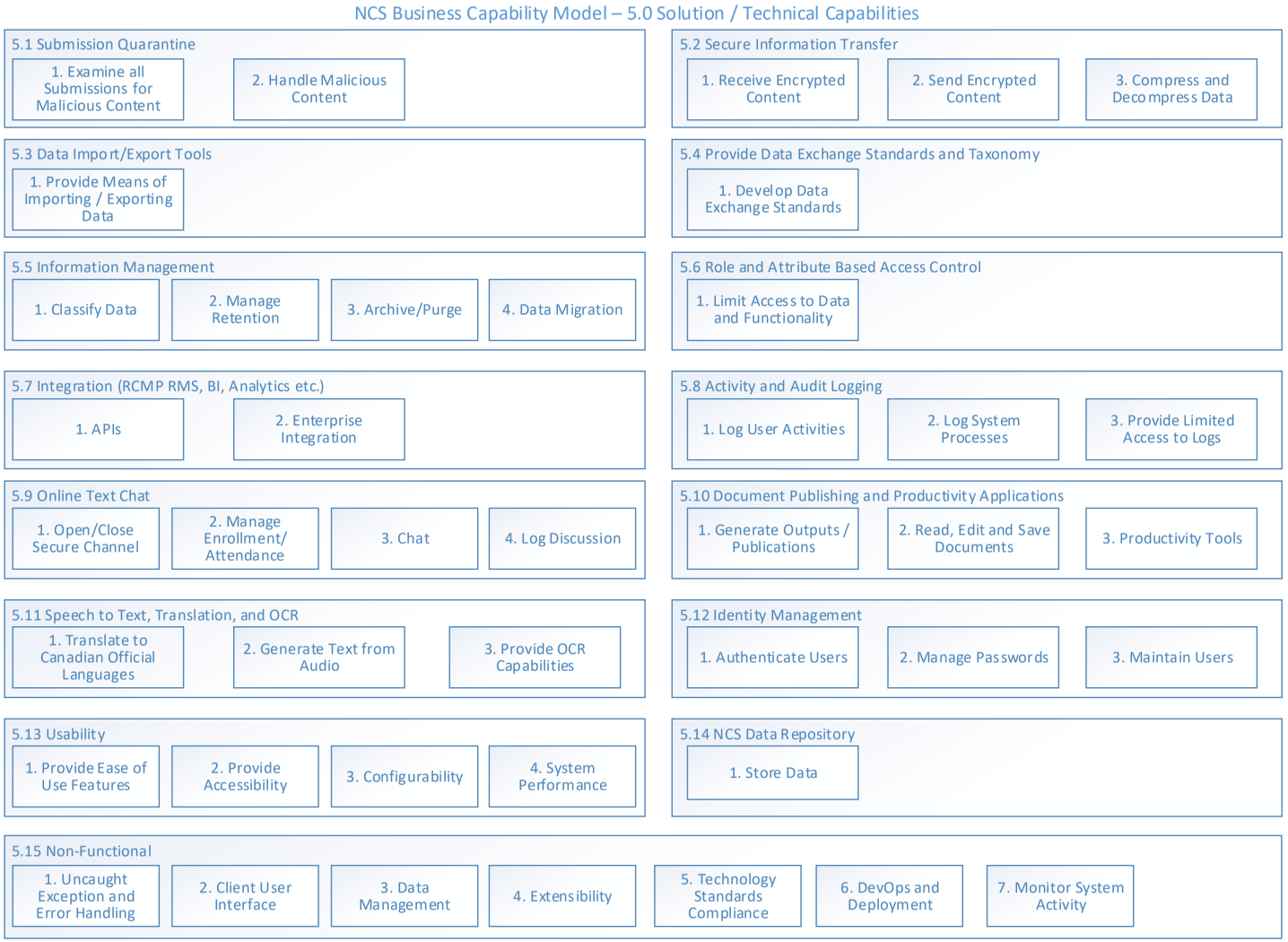


Figure C-6: NCS – Solution and Technical Capabilities

Table C-5: NCS BCM – Solution and Technical Capabilities

5.1 Submission Quarantine The Solution will scan all submissions (including data imported from physical media and large files) for malicious content, identify potentially malicious submissions and provide a means of reviewing these submissions prior to further processing.	
5.1.1. Examine all Submissions for Malicious Content	
5.1.1.1	The Solution must automatically examine all submissions (including attachments) to determine whether they contain any malicious content.
5.1.1.2	The Solution must store the results of screening for use in reviewing submissions deemed to be malicious.
5.1.1.3	The Solution must automatically ingest clean submissions for processing.
5.1.1.4	The Solution must hold for User review any submission that contains malicious content.
5.1.1.5	The Solution must scan for exploitive content. If found, the Solution must forward the submission to the National Child Exploitation Coordination Centre (NCECC). (Exploitive content could relate to exploitation of vulnerable persons)
5.1.1.6	The Solution must allow a User to forward exploitive content to the NCECC - in cases where the Solution has not automatically recognized the exploitive content.
5.1.2. Handle Malicious Content	
5.1.2.1	The Solution must provide a User with a means of reviewing submissions that have been identified as containing malicious content.
5.1.2.2	The Solution must allow a User to remove malicious attachments and ingest the modified submission.
5.2 Secure Information Transfer The Solution will be capable of securely transferring (receiving or sending) Information with Partners using Pretty Good Privacy (PGP) and x.509 open-source encryption standards.	
5.2.1. Receive Encrypted Content	
5.2.1.1	The Solution must be able to de-encrypt the received content for processing by the NCS (e.g. encrypted e-mails, attachments, files, digital signatures).
5.2.1.2	The Solution must ensure that the de-encrypted files do not contain any malicious content.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.2.1.3	The Solution must support RCMP and PGP open-source encryption standards.
5.2.2. Send Encrypted Content	
5.2.2.1	The Solution must be able to encrypt the outgoing content generated by the NCS or by a NC3 User.
5.2.2.2	The Solution must be able to send encrypted content (e.g. encrypted e-mails, attachments, files, digital signatures).
5.2.2.3	The Solution must support the use of Public keys to be verified and shared between the sender and receiver. X.509 and PGP must be supported.
5.2.2.4	The Solution must support the maintenance of public keys including storage on an encryption server at the RCMP for recovery and identification purposes.
5.2.2.5	The Solution must be integrated with Microsoft Outlook to provide a secure information sharing method eliminating clear text information.
5.2.3. Compress and Decompress Data	
5.2.3.1	The Solution must be capable of compressing data using standards such as, but not limited to .ZIP, .LZH.
5.2.3.2	The Solution must be capable of decompressing data using standards such as, but not limited to .ZIP, .LZH.
5.2.3.3	The Solution must support exchange of diary text, attachments, zipped and compressed files encrypted (not sent in the clear).
5.3 Data Import and Export Tools The Solution must be capable of ingesting and transferring data via physical media and electronically (e.g. on-line open source or internal data sources) including Large File (e.g. minimally > 1 Terabyte) Transfers.	
5.3.1. Provide Means of Importing and Exporting Data	
5.3.1.1	The Solution must be able to import and export data into and out of NCS (including existing data collected with the Initial Operating Capability solution).
5.3.1.2	The Solution must be able to export data via an Extract, Transform, and Load (ETL) capability either out of box or via other commercial platforms (e.g., IBM DataStage, open source products).
5.3.1.3	The Solution must be able to generate the exported file in a common format (e.g. XML, JSON) that can be imported by an external system (e.g. RMS, Analysis tools, MISP).
5.3.1.4	The Solution must be able to load reference and business data received in bulk (e.g. greater than 1 Terabyte) from Law Enforcement Agencies, Partners, Users, or Cybercrime Data Dictionary via both an API and a bulk interface.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.3.1.5	The Solution must be able to support the importation of data from physical media, email attachments, files transmitted via the P3, open source feeds, other LE portals (e.g. SIENNA, MISP), and data streams.
5.3.1.6	The Solution must provide a secure and safe means of managing all imported data including malware samples.
5.3.1.7	The Solution must provide the means to export selected NCS data to an RCMP-designated analytic tool or repository for analysis.
5.3.1.8	The Solution must provide the means to import analysis results to the NCS repository.
5.3.1.9	The Solution must provide the means to export selected NCS data to designated LE portals (e.g. SIENNA) or data sharing platforms (e.g. MISP).
5.3.1.10	The Solution must provide a means of subscribing to information sources (e.g. email or contact groups) to import email and discussion content.
5.4 Provide Data Exchange Standards and Taxonomy The system must be capable of exchanging data utilizing prescribed data exchange standards.	
5.4.1. Develop Data Exchange Standards	
5.4.1.1	The Solution must be able to exchange data with partner organizations using the cybercrime taxonomy (data exchange standards) developed by the NC3 and domestic and international partners.
5.4.1.2	The Solution must enable RCMP to define and maintain data exchange standards that can be used to for importing and exporting data into and out of NC3.
5.4.1.3	The Solution must support data exchange standards including, but not limited to: a. Structured Threat Information eXpression (STIX), b. Malware Information Sharing Platform (MISP); c. Vocabulary for Event Recording and Incident Sharing (VERIS); d. National Information Exchange Model (NIEM); e. Trusted Advance eXchange of Indicators Information (TAXII); and f. Law Enforcement Information Data Standard (LEIDS).
5.5 Information Management The system will be capable of managing the NC3 Information Lifecycle from information Receipt and Creation to Disposition. The NCS Data Repository will support the complete lifecycle of all information entities ingested or created as a result of processing cybercrime related submissions and service requests.	
5.5.1. Classify Data	

Table C-5: NCS BCM – Solution and Technical Capabilities

5.5.1.1	The Solution must be capable of using Data Categorizations such as Traffic Light Protocol and Government of Canada Information Security Designations, Europol Handling Codes (indicated by the data originator) to govern the sharing of information.
5.5.1.2	The Solution must validate that all data received contains or is labelled as per a data sharing handling and security designation codes.
5.5.1.3	The Solution must provide a User with a means of tagging and managing metadata for NC3 data assets. (e.g. a Data Cataloging)
5.5.1.4	The Solution must contain an indicator that a File contains a Subject (Suspect or victim) that is under the age of 18 ("Young Person Age"). The Young Person Age must be configurable.
5.5.1.5	The Solution must provide the ability to assign multiple categorizations to each piece of information (e.g. TLP= Red, Europol H3 and Government of Canada Protected B)
5.5.1.6	The Solution must provide a User with a means of editing the Data Categorization, TLP, Government of Canada Information Security Designations or Europol Handling Codes if necessary.
5.5.2. Manage Retention	
5.5.2.1	The Solution must manage data retention per configurable retention and disposition schedules and Dates applied by data originators.
5.5.2.2	The Solution must protect information and data from accidental loss and corruption (e.g., UI confirmation dialogs, referential integrity).
5.5.2.3	The Solution must allow a User to manually purge data based on approved expungement requests.
5.5.2.4	The Solution must allow a User to manually mark information as sequestered based on approved sequester requests.
5.5.2.5	The Solution must be capable of automatically notifying an authorized NC3 User, as well as providing the ability to relabel, export and purge information that has exceeded security designation of Protected B. (e.g. If a File has become a Protected C File)
5.5.3. Archive and Purge	
5.5.3.1	The Solution must be capable of using configurable time period parameters to automatically archive data to Cold Data Storage ("Archive").
5.5.3.2	The Solution must be capable of using configurable time period parameters to automatically set data retention period.
5.5.3.3	The Solution must purge information and data at the end of their associated retention period.
5.5.3.4	The Solution must identify information and data meeting archival criteria.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.5.3.5	The Solution must be capable of providing a data purge confirmation process to allow a User to approve the purge of data and edit the disposition date as necessary.
5.5.3.6	The Solution must take into account linkages when identifying data to purge. If a linkage exists, the linked data is subject to the retention date furthest in the future.
5.5.3.7	The Solution must be capable of retrieving data from Cold Data Storage into active ("Hot Storage").
5.5.4. Data Migration	
5.5.4.1	The Solution must be capable of accessing data that is collected during the Initial Operating Capability period.
5.5.4.2	The Solution must be capable of accessing data that is collected by the Canadian Anti-Fraud Centre (CAFC) and Public Reporting Website.
5.6 Role and Attribute Based Access Control Role Based Access and Attribute Based Access will be used to restrict access to functionality and data. RBAC and ABAC rules may be implemented to restrict access based on attributes such as User ID, Role or User Jurisdiction.	
5.6.1. Limit Access to Data and Functionality	
5.6.1.1	The Solution must limit availability of functionality to Users based on their assigned User Role(s).
5.6.1.2	The Solution must limit User's access to information including data, Files, and Projects per their User Role(s) and Attribute Based Access Controls (ABAC).
5.6.1.3	The Solution must support configurable User accounts and including flexibility to provide access to dashboards to various User levels.
5.7 Integration (RCMP RMS, BI, Analytics) The Solution will integrate with RCMP Corporate and select partner systems (e.g. RMS, Criminal Intelligence, Cybercrime Intelligence, Case Management) including Call-Centre Computer Telephony integration, using Open source standards where applicable.	
5.7.1. APIs	
5.7.1.1	The Solution must make use of Application Programming Interfaces (API)s that adhere to the Government of Canada Standards on APIs for system integrations between components, tools used by the NC3 and external platforms.
5.7.1.2	The Solution must be capable of supporting the exchange of data using APIs with external systems and report across multiple information domains such as; Police Records Management Systems, Other Government Departments or other Cybercrime Partners (e.g. Cybersecurity Firms, Financial Institutions).

Table C-5: NCS BCM – Solution and Technical Capabilities

5.7.1.3	The Solution must integrate with the RCMP corporate email system in order to ingest submissions and service requests, allow Users to communicate with cybercrime partners.
5.7.1.4	The Solution must provide the ability to invoke external synchronous web service APIs via open industry standards when the authoritative source of that data and functionality resides in other systems.
5.7.1.5	The Solution must, for all APIs, be able to expose data as non-proprietary business entities or object schemas. Specifically, APIs must be able to abstract raw back end table and data structures.
5.7.2. Enterprise Integration	
5.7.2.1	The Solution must be capable of utilizing an Event Handler to manage all interactions between components within the Solution, using asynchronous event messaging.
5.7.2.2	The Solution must be capable of utilizing a dedicated cloud connection to ensure a secure high-speed connection exists between the RCMP data centre and the RCMP Protected B Cloud Tenant.
5.7.2.3	The Solution must integrate with 3rd party enterprise data governance management tools.
5.7.2.4	The Solution must integrate with 3rd party Geospatial services.
5.7.2.5	The Solution must expose all APIs via open standard bindings and protocols (including but not limited to: Representational State Transfer (REST) with JavaScript Object Notation (JSON) and Extensible Markup Language (XML).
5.7.2.6	The Solution must support Transport Layer Security (TLS) 1.2 encryption for all interfaces as a minimum level of connectivity security.
5.8 Activity and Audit Logging The Solution must record all User and system activities in activity logs. System activity will be recorded in system audit logs.	
5.8.1. Log User Activities	
5.8.1.1	The Solution must retain an activity log of all activity performed by a P3 and NC3 User including adding, modifying, querying, printing, exporting and deleting information.
5.8.1.2	The Solution must enable the NC3 User to create a manual activity that would not otherwise be recorded by the system activity log. (e.g. File related phone call, OS Search)
5.8.1.3	The Solution must ensure that activity log files are immutable.
5.8.1.4	The Solution must ensure that logs contain the User id, the activity date and time and the action that was performed.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.8.1.5	The Solution must record the query parameters used to query the NCS Cyber Repository.
5.8.1.6	The Solution must maintain all versions of a file if it is manipulated during intelligence extraction activities.
5.8.1.7	The Solution must log all query search criteria and the subsequent result sets.
5.8.2. Log System Processes	
5.8.2.1	The Solution must retain a log of all activities performed automatically by the system.
5.8.2.2	The Solution must retain an audit log of all activities performed on any Solution database.
5.8.2.3	The Solution must retain an audit log of all User access to the system (e.g. who logged in, login time, logout time, attempted login)
5.8.2.4	The Solution must ensure that audit log files are read-only and immutable.
5.8.2.5	The Solution must be capable of raising notifications to admin Users based on system component failure or repeated User attempts resulting in error messages.
5.8.2.6	The Solution must provide interfaces that effectively handle situations where external systems experience failure or are unavailable.
5.8.3. Provide Limited Access to Logs	
5.8.3.1	The Solution must enable authorized NC3 Users to view the contents of the User activity log files.
5.8.3.2	The Solution must enable authorized Users (e.g. system administrators) to view the contents of the system audit log files.
5.9 Online Text Chat The system will provide a Secure Real-time text-based Chat feature for NC3 and P3 Users. This includes Users of NC3 that are geographically separated from the main NC3 Office (e.g. J-Cat).	
5.9.1. Open and Close Secure Channel	
5.9.1.1	The Solution must allow a User to open and close a secure channel to initiate and end a chat.
5.9.1.2	The Solution must allow a Chat Administrator to invite other NC3 Users to join a chat.
5.9.2. Manage Enrollment and Attendance	
5.9.2.1	The Solution must notify invited Users of a Chat to which they are invited. The User must be permitted to accept or reject the invitation.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.9.2.2	The Solution must allow invited Users to join or leave a chat to which they are invited.
5.9.2.3	The Solution must allow the Chat administrator with the ability to view a User list of who is currently signed into the Chat.
5.9.3. Chat	
5.9.3.1	The Solution must support secure exchange of text messages (group chat), voice and video conference.
5.9.3.2	The Solution must allow links to be included in chat texts. E.g. links to Files, Projects.
5.9.4. Log Discussion	
5.9.4.1	The Solution must store an immutable record of all content entered by chat participants.
5.10 Document Publishing and Productivity Applications The business will require the ability to output the contents of Tickets, File and Projects in electronic as well as hardcopy formats. The business also requires the ability to use "Office Productivity" software such as word processing or spreadsheet software to examine attachments or edit content for outputs. The system must be capable of seamlessly allowing Users to open such attachments or transfer information between attachments and the system.	
5.10.1. Generate Outputs and Publications	
5.10.1.1	The Solution must enable Users to edit and format documents to publish using word processing tools.
5.10.1.2	The Solution must be capable of assembling the components of a product or email (including secure email) for review by a User.
5.10.1.3	The Solution must be capable of creating standard format PDFs (e.g. Data Preservation Demands or Orders), attaching them to emails and queueing the email for review and issuance by a User.
5.10.1.4	The Solution must be capable of producing related Data Preservation Demand and Data Preservation Order Forms 5.001, 5.002, 5.003, 5.009.
5.10.1.5	The Solution must be capable of allowing a User to create and send an email (including a secure email) to a cybercrime partner.
5.10.1.6	The Solution must automatically mark documents per the data security categorization e.g. Government of Canada levels of security (Protected A, B, C, Confidential, Secret and Top Secret), the Europol Handling Codes (H1, H2, and H3) and Traffic Light Protocol (White, Green, Amber and Red) and let Users override if required.
5.10.2. Read, Edit and Save Documents	
5.10.2.1	The Solution must allow a User to open and view an attachment with the appropriate reader.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.10.2.2	The Solution must provide a "save as" capability that will allow for the conversion of a file from one type to another (e.g. Word document to PDF).
5.10.2.3	The Solution must provide a spell checker feature, minimally in Canadian English and French.
5.10.3. Productivity Tools	
5.10.3.1	The Solution must provide a tool to allow a User to calculate monetary values from any currency to Canadian Dollars or US Dollars on the date that the transaction was entered into the system.
5.10.3.2	The Solution must provide a secure real-time collaboration environment that supports real-time concurrent access, modification, review, feedback and discussion of Tools, Projects and artifacts by authorized NC3 Users or P3 Users. Artifacts may include, but are not limited to, text documents, spreadsheets, PDF, presentations, or visualization maps.
5.10.3.3	The Solutions Collaboration capability must be capable of maintaining the history and integrity of prior revisions.
5.10.3.4	The Solutions Collaboration capability must provide a User with the ability to display and demonstrate tools and artifacts through screen sharing.
5.11 Speech to Text, Translation, and OCR The business requires the ability to convert audio files to text, translate text files to English and French and convert images of printed or handwritten text into machine usable data.	
5.11.1. Translate to Canadian Official Languages	
5.11.1.1	The Solution must be able to translate text from English to French and vice versa in accordance with GC standards.
5.11.1.2	The Solution must be able to translate text from other languages to English or French. List of supported languages to be determined (e.g. Russian, Spanish, Cantonese, Mandarin, Korean, Hindi, Farsi, German).
5.11.1.3	The Solution must store the translated text as part of the associated NCS file.
5.11.1.4	The Solution must retain the original text in the originating language.
5.11.1.5	The Solution must provide an option to display translated (to English or French) data when a user is viewing a File containing foreign languages.
5.11.2. Generate Text from Audio	
5.11.2.1	The Solution must be able to generate text from audio files.
5.11.2.2	The Solution must store the generated text as part of the associated NCS file.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.11.2.3	The Solution must retain the original audio file as part of the associated NCS file..
5.11.3. Provide OCR Capabilities	
5.11.3.1	The Solution must provide a means of converting images of printed or handwritten text into machine usable data.
5.11.3.2	The Solution must provide a means of scanning and reading QR (Quick Response) Codes in order to use the data contained in them. For example QR Codes on Bitcoin "Tickets" or Gift Cards.
5.12 Identity Management The creation, management and maintenance of User Identities (Username and Password) is required to manage access to the Solution. These requirements are highly regulated by the RCMP environment and Departmental Security Branch.	
5.12.1. Authenticate Users	
5.12.1.1	The Solution must provide login (Authentication) functionality per RCMP approved identity management standards and technologies; including to the P3.
5.12.1.2	The Solution must verify the identity of a User at login to subsequently enforce RBAC requirements within the Solution.
5.12.2. Manage Passwords	
5.12.2.1	The Solution must provide Users with the ability to manage their passwords. Password management must comply with RCMP standards (e.g. format, periodic reset).
5.12.2.2	The Solution must use Azure Active Directory.
5.12.3. Maintain Users	
5.12.3.1	The Solution must allow an authorized User to view, create, modify profile, suspend or reinstate a User of the NCS system or the P3.
5.12.3.2	The Solution must allow an authorized RCMP User to assign or revoke an established access role to a User.
5.12.3.3	The Solution must allow an authorized RCMP User to verify the identity of new users and manage their public and private keys (PGP and x.509), whether assigned to, or supplied by the User.
5.13 Usability Incorporates capabilities related to the ease of use, accessibility, on-line help, access to second level help and performance.	
5.13.1. Provide Ease of Use Features	

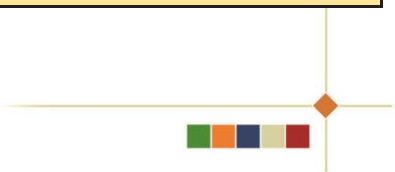


Table C-5: NCS BCM – Solution and Technical Capabilities

5.13.1.1	The Solution must adhere to applicable Government of Canada IT system usability standards for accessibility and common look and feel. These standards are derived from Web Content Accessibility Guidelines (WCAG) 2.0 Standards. The Solution must comply with Web Accessibility standards as described in TBS Standard on Web Accessibility[3].
5.13.1.2	The Solution must provide a User customizable User Interface (e.g., windows layout, dashboards, work queues, default language selection).
5.13.1.3	The Solution must provide User Interfaces with meaningful; sequences, information relationships, focus, messages, consistent look and feel, screen labels, consistent navigation and orientation + User warnings.
5.13.1.4	The Solution must provide Users with access to context sensitive on-line help.
5.13.1.5	The Solution must make use of searchable data selection lists and auto-fill controls and data widgets to ease data capture and standardize data entry.
5.13.1.6	The Solution must make maximum use of available data (such as Partner Data) to minimize user data entry and maximize accuracy.
5.13.1.7	The Solution must allow a User to create a Help Ticket for assistance from NCS system support resources. Help Tickets can be escalated to Central Help-Desk for resolution.
5.13.2. Provide Accessibility	
5.13.2.1	The Solution must provide all User interfaces, documentation and support in both of Canada's official languages (English and French). This means Users selecting French as their language will not see anything in English in the Solution's GUI, including but not limited to help files, tutorials, error messages and legal information. (User-generated content is excluded).
5.13.2.2	The Solution must be available and accessible to individuals with disabilities, compliant with WCAG 2.0 A accessibility standards.
5.13.2.3	The Solution must be provided to Users at locations across Canada and Internationally.
5.13.3. Configurability	
5.13.3.1	The Solution must provide authorized Users with the ability to maintain configurable parameters (e.g. data selection lists, business rules, templates).
5.13.3.2	The Solution must, to the extent possible, allow configuration without incurring system downtime or new software releases.
5.13.4. System Performance	

[3] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

Table C-5: NCS BCM – Solution and Technical Capabilities

5.13.4.1	The Solution must allow at least 500 concurrent Users to use the NCS and P3 without a degradation in performance.
5.13.4.2	The Solution must be capable of managing data concurrency when more than one User is accessing the same file and data at the same time.
5.14 NCS Data Repository The NCS Data Repository will contain all NC3 Operational data including all submissions and service requests received, related metadata and resulting digital artifacts and business products.	
5.14.1. Store Data	
5.14.1.1	The Solution must provide a Data Repository that is capable of securely storing all submissions, service requests, attachments, metadata, work and analysis tasks and results, activity and audit logs and work products related to work performed by the NCS system and NC3 Users
5.14.1.2	The Solution must store data in a secure manner in accordance with TBS Standards.
5.14.1.3	The Solution must be capable of storing data that is received in multiple languages retaining the submissions character set. (e.g. In addition to French and English - store Russian, Spanish, Cantonese, Mandarin, Korean, Hindi, Farsi, German)
5.14.1.4	The Solution must ensure that all data processed, stored, maintained, derived and utilized by the Solution, including all online storage as well as data backups and archived data, reside in Canada.
5.14.1.5	The Solution must be capable of handling both structured and unstructured data formats.
5.14.1.6	The Solution must be elastic and scalable to handle the potential for increasing or decreasing volumes of cybercrime transactions and data.
5.14.1.7	The Solution must protect information and data from unauthorized action and access
5.14.1.8	The Solution must protect information and data from accidental loss and corruption.
5.15 Non-Functional The following capabilities include non-functional requirements related to User Interface, Data Management, adherence to GC Standards and system monitoring.	
5.15.1. Uncaught Exception and Error Handling	
5.15.1.1	The Solution must capture all uncaught run-time exceptions and dead-letter queue messages generated during NCS business transaction processing.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.15.1.2	To support error analysis, the Solution must include message Correlation Ids to facilitate the tracking and logging of events through the system.
5.15.1.3	The Solution must include a secure User search facility so that system administrators can examine and update the error list once errors are resolved.
5.15.2. Client User Interface	
5.15.2.1	The Solution must provide a browser-based client as its user interface that is compatible at a minimum with: 64-bit Microsoft Internet Explorer v11 and higher, Microsoft Edge, Firefox, and 64-bit Google Chrome v75 and higher.
5.15.2.2	The Solution must provide a single-sign on that allows NC3 Users and P3 Users access to the scope of their RBAC functionality without multiple logins.
5.15.2.3	The client application must automatically timeout after a configurable time of inactivity, at which time re-authentication is required.
5.15.2.4	The Solution must protect information through secure authentication methods using open standards (including but not limited to OpenID, OAuth, or SAML).
5.15.2.5	The Solution must provide a busy notification (e.g. hourglass) when the software is busy performing an operation and the user must wait.
5.15.3. Data Management	
5.15.3.1	The Solution must auto-tag data as it is ingested to the NCS to maintain data provenance (e.g. time stamp, data provider source, and other metadata useful for auditing or monitoring purposes).
5.15.3.2	The Solution must capture and retain data lineage and provenance metadata throughout data transformations and data integration processes in accordance with Government of Canada's Standard on Metadata.
5.15.3.3	The Solution must include data validation and data quality monitoring functions for batch, real-time, and near-real time data capture processes.
5.15.3.4	The Solution must provide interfaces for data cleansing validation using standardized source information (e.g. postal addresses, geocoding, demographic data, RCMP data standard).
5.15.3.5	The Solution must support data federation by providing virtual access to database structures, including semi-structured data and the ability to join data across data sources for real-time access and analysis.
5.15.3.6	The Solution must support query optimization, both automatically as part of DBMS requests, and manually within the advanced internal optimization of manually created queries.

Table C-5: NCS BCM – Solution and Technical Capabilities

5.15.4. Extensibility	
5.15.4.1	The Solution must provide an admin User the capability to customize user interface functionality (e.g., adding entities, attributes, and logic) using a low-code or no-code approach.
5.15.5. Technology Standards Compliance	
5.15.5.1	The Solution must adhere to GC API guidelines as defined by Government of Canada Standards on APIs[4].
5.15.5.2	The Solution must adhere to GC RBAC and ABAC standards and guidelines. See User Authentication Guidance for Information Technology Systems (ITSP.30.031 v3)[5].
5.15.6. DevOps and Deployment	
5.15.6.1	The Solution applications must be packaged in Containers of one or more Microservices with parameterized scripts that can be tailored for each target environment (e.g. Quality Control (QC), Production).
5.15.6.2	Every release must include documentation of all scripts and changes.
5.15.6.3	Installation and build scripts must be in a code readable format and deployed as a package to build the Solution in the appropriate environment.
5.15.6.4	Update and patch scripts must be in a code readable format and in a package format to be deployed as an application update.
5.15.6.5	Each component to be installed on a different server must have its own build script in a code readable format.
5.15.6.6	Each release must adhere to the RCMP's code repository requirements and release methodology.
5.15.7. Monitor System Activity	
5.15.7.1	The Solution must enable the monitoring of logins, database size, database access, CPU usage, cloud resource usage and network traffic.
5.15.7.2	The Solution must provide System and Security Event Logging.
5.15.7.3	The Solution must store all activity and system logs using the RCMP Protected B Cloud Tenant logging services.

[4] https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html

[5] http:://cyber.gc.ca/en/guidance/user-authentication-guidance-information technologysystems-itsp30031-v3

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915	-	155 XL
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
M7594-205915	155xl M7594-205915	

Appendix D – High-Level Architecture Diagram

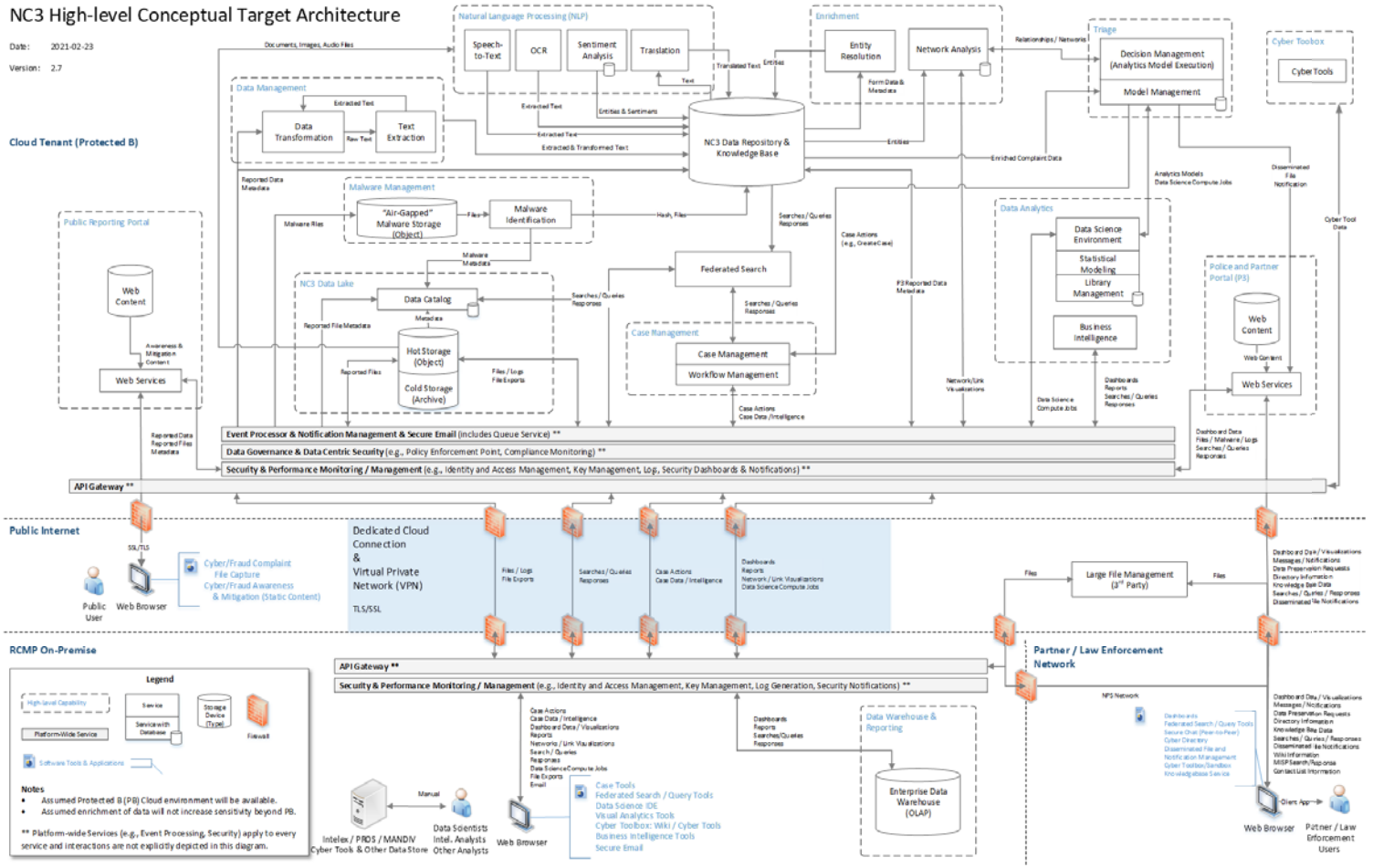


Figure D-1: NCS High Level Architecture

D.1 Target Architecture Component Descriptions

a) Several of the universal components of the Solution are depicted at a high-level to increase readability and reduce the complexity of the diagram, specifically:

   i) API Gateway;

   ii) Security & Performance Monitoring and Management;

   iii) Data Governance & Data Centric Security; and

   iv) Event Processor & Notification Management & Secure Email.

b) It is expected that these universal components will integrate and interact with nearly every component of the Solution; thus, they are depicted as a stack. These are also considered to be the more complex aspects of the Solution and have been left to the Contractor to determine the best way to deliver this functionality while adhering to the requirements.

c) A description of each component of the Target Architecture is included in Table D-1: Architecture Component Descriptions for reference.

Table D-1: Architecture Component Descriptions

Architectural Component	Description
Public Reporting Portal - Web Services	This component will be developed outside of the Contractor Solution, and is included on the diagram because it will interface with the Solution, see Section 4.4 – Public Reporting Web site for more information. This RCMP-developed component provides browser-based access and a mobile phone app to capture cyber and fraud complaint information from private individuals and small or medium-sized businesses (SMB). It provides a central, public-facing portal for the Canada-wide collection of cybercrime and fraud complaints from private individuals and SMB.
P3 - Web Content	This component provides access to cybercrime-related directories, the NC3 Knowledge Base, and a catalogue of NC3 tools and services.
P3 - Web Services	This component provides secure two-way communication between the RCMP and trusted cybercrime Partners. The P3 facilitates the submission and capture of cybercrime-related service requests and submissions by trusted Partners to the NCS. In addition, issuing notifications to trusted Cybercrime Partners will be a key capability of the P3. Potential P3 Users include Canadian Law Enforcement agencies, other government departments (e.g., Canadian Centre for Cyber Security (CCCS), Canadian Radio and Television Commission (CRTC), and Statistics Canada), and RCMP Cybercrime Liaison Officers.
Decision Management	This component provides an automated mechanism for generating decisions based on conditions (e.g., models and rules). It allows for defining and executing logic rules, executing analytics models in parallel, and performing ensemble voting for decision support.
Model Management & Compute	This component manages and executes analytics models to support various functions for the Decision-Management component. It deploys and retires models, provides versioning, and tracks the performance (e.g., effectiveness and errors) of models in production throughout their life cycle.

Table D-1: Architecture Component Descriptions

Architectural Component	Description
Entity Resolution	This component provides automated disambiguation, consolidation, identification, and management of real-world entities (e.g., people, places, and things) using the linking or grouping of like data elements based on a set of predefined rules.
Network Analysis	This component identifies and tracks links and networks between resolved real-world entities (e.g., people, places, and things). It provides a mechanism for determining the risk associated with a particular entity based on associations with other entities in the same network. These links and networks are displayed using a separate tool for diagramming and displaying networks and links between the entities.
Data Transformation	This component provides data conversion, cleansing, and integration services to transform data from one format to another and prepare it for storage and use. It also provides the mechanisms for ingesting data from various sources (e.g., data feeds, physical media, and large files).
Text Extraction	This component extracts text and data from various sources (e.g., documents, tables, and form fields) and makes it readily available for use.
Sentiment Analysis	This component computationally identifies, categorizes, and scores opinions expressed in a passage of text in order to determine the author's attitude towards a particular topic as being positive, negative, or neutral.
Case Management	This component provides central management abilities for cases. Cases are files which group-related data on a topic of interest (e.g., client) including, but not limited to, notes, communications, history, contact information, analyses, and findings. This component also tracks and manages the state of each case (e.g., new, assigned, and closed) as well as facilitates the User who is conducting various actions within a case (e.g., assignment, priority elevation) in conjunction with the Workflow Management component.
Workflow Management	This component provides the mechanism for managing tasks as well as the logic to direct flow between tasks. It may be used for coordinating Tickets for submissions and intelligence files which make up cases. This includes scheduling, coordinating, and executing steps in sequence or parallel to accomplish a task. It also includes triggering events (e.g., notifications), managing points of manual work required from a User, and generating work lists for review.
Malware Identification	This component will scan all submissions—including data imported from physical media and large files—for malicious content, identify potentially malicious submissions, and provide a means of reviewing these submissions prior to further processing. This component also provides the ability to cross-reference malware samples from Canadian Law Enforcement against a national repository of police-submitted malware reports as well as selected domestic and international malware solutions.

Table D-1: Architecture Component Descriptions

Architectural Component	Description
Malware Storage (Object)	This component stores the malware sample in an isolated or quarantined, segregated environment from other files that are handled by the Solution. As closely resembling an air gapped-solution as possible. The Solution needs to ensure that malware samples do not compromise the security or integrity of the RCMP network.
Statistical Modeling	This component provides the ability to perform advanced ad-hoc statistical analysis and modeling of data.
Library Management	This component provides the ability to manage versions of packages and dependencies (e.g., Python libraries) for development and deployment within the Data Science Environment. This component may be a function of the Data Science Environment or it may be a stand-alone component.
Data Science Environment	This component provides Users with a safe, secure, and isolated environment (i.e., Sandbox) in which to apply advanced analytics tools and techniques. It supports Users working with common and popular data science languages (e.g., Python, Scala, and Java), documenting techniques (e.g., markup), executing and deploying models, and visualizing results all within a single environment (e.g., notebook).
Cyber Tools	This component provides Users with access to Cyber Tools (e.g. Virtual Currency Tracking, IP Lookup, PCAP Analysis). Some tools are on premise while some may be available as SaaS services.
Visual Analytics Tools	This component provides the ability to visually graph and diagram, analyze, investigate, manipulate, and manage data. Visualizations enable the User to gain rapid insights into data and may include link charts, event charts, geospatial maps, and other graphical depictions (e.g., StoryMaps) that are generated through analytics techniques.
Business Intelligence	The component provides automated analyses and visualizations of data to support decisions. It derives performance and summary metrics from data and allows the User to schedule the generation of automated reports and dashboards based on predetermined areas of interest.
Speech-to-Text	This component automatically derives text from audio speech files.
Optical Character Recognition (OCR)	This component extracts text from images including printed or handwritten characters.
Translation	This component provides translation of text between different languages. At a minimum, it is used to translate text from English to French and vice versa.
NC3 Data Repository and Knowledge Base	This component provides a central mechanism for managing all of the NC3 operational data including all submissions, raw and cleansed data, service requests, as well as related metadata and the resulting digital artifacts and business products. This includes a central hub of searchable information on Cyber investigation topics and techniques.

Table D-1: Architecture Component Descriptions

Architectural Component	Description
Data Catalog	This component provides fully automated and scalable, metadata management capabilities to enable Users to quickly discover and manage their data. It automates the tracking of objects in the Hot Storage (i.e., Object) and Cold Storage (i.e., Archive) components and makes the corresponding metadata readily available for queries through the Federated Search component.
Hot Storage (Object)	This component provides the ability to store and retrieve frequently accessed data as objects in any format (e.g., documents, images, audio, and video) with very low latency.
Cold Storage(Archive)	This component provides the ability to perform the long-term, redundant storage and retrieval of infrequently-accessed data in any format (e.g., documents, images, audio, and video).
Federated Search	This component provides Users with the ability to search for and retrieve information from NC3 data sources in a variety of formats using a single point query. An advanced query must also be available to provide faceted search and content drill-down functionality.
Compliance Monitoring	This component provides management and tracking of data assets throughout the NC3 information life cycle (i.e., Receipt and Creation to Destruction and Archiving) to ensure compliance with government and industry standards and policies.
Policy Enforcement Point	This component provides the capability to manage role-based access to information assets. It restricts access to functionality based on User attributes (e.g., username, role, or jurisdiction).
Identity and Access Management	This component provides the ability to manage access to resources—whether through web interfaces or programmatically—using permissions and policies. It manages User identities (e.g., usernames, passwords, and access keys), roles, and groups as well as identity federation and Multi-Factor Authentication (MFA).
Key Management	This component allows an authorized NC3 User to manage the issuance and revocation of public and private keys in the public key infrastructure that is leveraged by the Solution.
Log Management	This component records all User and system activities in read-only activity logs to provide an auditable record for compliance, performance, analytics, and security purposes.
Security & Performance Monitor	This component provides real-time system monitoring capabilities including system resource and network monitoring. It works in conjunction with the Log Management component to analyze logs, derive metrics, and generate notifications to the System Administrators using the Notification Management component.

Table D-1: Architecture Component Descriptions

Architectural Component	Description
Application Programming Interface (API) Gateway	This component provides an API-management solution that allows developers to create, publish, maintain, monitor, and secure APIs across the Solution. It encourages the loose coupling of components and supports integration with RCMP corporate assets as well as select Partner systems using open standards.
Queuing Service	This component provides a message-queuing service to support the loose coupling of components, work queues, and notifications. It works in conjunction with the Event Hander component for managing triggers and message delivery.
Notification Manager	This component provides functionality to support the management of User notifications including the lists of authorized publishers and subscribers. It responds to event triggers, takes into account disclosure rules and display, and manages notifications for implicated Users. It works in conjunction with the Event Handler and Queueing Service components for managing the delivery of notifications.
Event Handler	This component asynchronously manages all messaging and interactions between components within the Solution based off of event triggers. It provides a centralized mechanism to ensure that services are co-ordinated to perform complex tasks.
Secure Email	This component provides the ability to decrypt incoming secure emails as well as create and send secure (i.e., encrypted) emails within the P3 and other partner portals.
Dedicated Cloud Connection	This component provides a secure, dedicated, high-speed connection between the RCMP data centre and the RCMP Protected B Cloud Tenant.
Virtual Private Network (VPN)	This component provides a secure, private communication network across the public Internet between On-Premises RCMP assets and the RCMP Protected B Cloud Tenant.
Large File Management	This component provides the ability for the RCMP and Partner organizations to securely upload and manage large files in a secure and accessible location.
Secure Chat (Peer-to-Peer)	This component provides secure, real-time, text-based communication between NC3 and P3 Users including the logging of Users and logging the date and time of the chat session.

APPENDIX E – SECURITY REQUIREMENTS TRACEABILITY MATRIX

a) The NCS Security Requirements Traceability Matrix (SRTM) lists the security controls that must be included as part of the Solution. The table below lists the security control Identification (ID) along with the name, the assigned responsibility for the control and the division of responsibility if shared between the RCMP and Contractor as a multi-part control. For details of the control, refer to Annex 3A - Security Control Catalogue (ITSG-33)[1] on the Canadian Centre for Cyber Security website.

a) The right-most column of Table E-1 entitled **Enhancements Assigned to Contractor** lists those control enhancements described in ITSG-33 which are designated as the responsibility of the Contractor to fulfill. Where an enhancement is shown to be "Shared", the RCMP and Contractor shall be jointly responsible for fulfilling that enhancement.

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
AC-1	Access Control Policy and Procedures	Shared		
AC-2	Account Management	Shared		AC-2(1) - Shared AC-2(2) - Shared AC-2(3) - Shared AC-2(4) - Shared AC-2(5) - Shared AC-2(7) - Shared AC-2(9) - Shared AC-2(10) - Shared AC-2(11) AC-2(12) AC-2(13)
AC-3	Access Enforcement	Shared		
AC-4	Information Flow Enforcement	Contractor		AC-4(21)
AC-5	Separation of Duties	Shared	a) Shared b) Contractor	

[1] https://cyber.gc.ca/en/guidance/annex-3a-Security-control-catalogue-itsg-33

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
			c) Contractor	
AC-6	Least Privilege	Shared		AC-6(1) - Shared AC-6(2) - Shared AC-6(3) - Shared AC-6(5) - Shared AC-6(7) - Shared AC-6(8) - Shared AC-6(9) - Shared AC-6(10) - Shared
AC-7	Unsuccessful Login Attempts	Shared		
AC-8	System Use Notification	Shared		
AC-9	Previous Logon (Access) Notification	Contractor		AC-9 (1)
AC-10	Concurrent Session Control	Shared		
AC-11	Session Lock	Shared		AC-11(1) - Shared
AC-12	Session Termination	Shared		AC-12(1)
AC-14	Permitted Actions Without Identification or Authentication	Shared		
AC-17	Remote Access	Shared		AC-17(1) AC-17(2) - Shared AC-17(3) - Shared AC-17(4) AC-17(9) AC-17(
AC-18	Wireless Access	Shared		AC-18(1) - Shared AC-18(5)

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
AC-19	Access Control for Mobile Devices	Shared		AC-19(4) AC-19(5)
AC-20	Use of External Information Systems	Shared		AC-20(1) - Shared AC-20(2) - Shared
AC-21	User-Based Collaboration and Information Sharing	Shared	A) Contractor B) RCMP	
AC-22	Publicly Accessible Content	Shared		
AC-23	Data Mining Protection	Contractor		
AC-24	Access Control Decisions	Shared		
AT-1	Security Awareness and Training Policy and Procedures	Shared		
AT-2	Security Awareness	Shared		AT-2(1) - Shared AT-2(2) - Shared
AT-3	Role Based Security Training	Shared		AT-3(1) AT-3(2) AT-3(3)
AT-4	Security Training Records	Shared		
AU-1	Audit and Accountability Policy and Procedures	Shared		
AU-2	Auditable Events	Shared	A) Contractor B) RCMP C) RCMP D) RCMP	AU-2(3) - Shared
AU-3	Content of Audit Records	Shared		AU-3(1) - Shared AU-3(2) - Shared

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
AU-4	Audit Storage Capacity	Contractor		
AU-5	Response To Audit Processing Failures	Shared		AU-5(1) AU-5(2)
AU-6	Audit Review, Analysis and Reporting	Shared		AU-6(1) - Shared AU-6(3) - Shared AU-6(10) - Shared
AU-7	Audit Reduction and Report Generation	Shared		AU-7(1) - Shared
AU-8	Time Stamps	Contractor		AU-8(1)
AU-9	Protection of Audit Information	Shared		AU-9(2) AU-9(3) AU-9(4) - Shared
AU-10	Non-Repudiation	Contractor		
AU-11	Audit Record Retention	Shared		
AU-12	Audit Generation	Contractor		AU-12(2)
AU-14	Session Audit	Contractor		AU-14(1)
CA-1	Security Assessment and Authorization Policies and Procedures	Shared		
CA-2	Security Assessments	Shared	A) RCMP B) Shared C) RCMP D) RCMP	CA-2(1) - Shared CA-2(2) - Shared CA-2(3)
CA-3	Information System Connections	Shared		CA-3(3) - Shared CA-3(5) - Shared

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
CA-5	Plan of Action and Milestones	Contractor		
CA-6	Security Authorization	RCMP		
CA-7	Continuous Monitoring	Shared	A) RCMP B) Contractor for tooling, RCMP for operations C) RCMP D) RCMP E) RCMP F) RCMP G) RCMP	CA-7(1) - Shared
CA-8	Penetration Testing	Contractor		CA-8(1)
CA-9	Internal System Connections	Shared	A) RCMP B) Contractor	
CM-1	Configuration Management Policy and Procedures	Shared		
CM-2	Baseline Configuration	Shared		CM-2(1) - Shared CM-2(2) - Shared CM-2(7) - Shared
CM-3	Configuration Change Control	Shared	A) RCMP B) RCMP C) RCMP D) Contractor E) Contractor F) Shared G) Shared	CM-3(1) - Shared CM-3(4) CM-3(6)
CM-4	Security Impact Analysis	Shared		

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
CM-5	Access Restrictions for Change	Shared		CM-5(1) CM-5(3) CM-5(5) - Shared CM-5(6)
CM-6	Configuration Settings	Shared	A) Contractor B) Contractor C) Shared D) Shared	CM-6(1) CM-6(2) - Shared
CM-7	Least Functionality	Contractor		CM-7(1) - Shared CM-7(2) CM-7(5) - Shared
CM-8	Information System Component Inventory	Contractor		CM-8(1) CM-8(2) CM-8(3) CM-8(5)
CM-9	Configuration Management Plan	Shared		
CM-10	Software Usage Restrictions	Shared	A) Contractor B) Contractor C) N/A	CM-10(1) - Shared
CM-11	User Installed Software	Shared	A) RCMP B) Contractor C) RCMP	
CP-1	Contingency Planning Policy and Procedures	Shared		
CP-2	Contingency Plan	Shared	A) Shared a) RCMP	CP-2(1) - Shared CP-2(2)

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
			b) RCMP c) RCMP d) Contractor e) Contractor f) RCMP B) Contractor C) RCMP D) Shared E) Contractor F) Contractor G) Shared	CP-2(3) - Shared CP-2(6) - Shared CP-2(8) - Shared
CP-3	Contingency Training	Contractor		
CP-4	Contingency Plan Testing and Exercises	Shared		CP-4(1) - Shared
CP-6	Alternate Storage Site	Contractor		CP-6(1) CP-6(3)
CP-7	Alternate Processing Site	Contractor		CP-7(1) CP-7(2) CP-7(3) CP-7(4)
CP-8	Telecommunications Services	Contractor		CP-8(1) CP-8(2) CP-8(3)
CP-9	Information System Backup	Shared	A) Contractor B) Contractor C) Contractor D) Contractor	CP-9(1) - Shared CP-9(3) - Shared CP-9(5) CP-9(7) - Shared

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
			AA) RCMP	
CP-10	Information System Recovery and Reconstitution	Contractor		CP-10(2) - Shared
IA-1	Identification and Authentication Policy and Procedures	Shared		
IA-2	Identification and Authentication (Organizational Users)	Contractor		IA-2(1) IA-2(2) IA-2(3) IA-2(4) IA-2(5) IA-2(6) IA-2(8) IA-2(11)
IA-3	Device Identification and Authentication	Contractor		
IA-4	Identifier Management	Shared	A) RCMP B) RCMP for USER; Contractor for system accounts C) RCMP for USER; Contractor for system accounts D) RCMP for USER; Contractor for system accounts E) RCMP	IA-4(4) - Shared
IA-5	Authenticator Management	Shared		IA-5(1) - Shared IA-5(2) - Shared IA-5(3) - Shared IA-5(4) - Shared

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
				IA-5(6) - Shared IA-5(7) - Shared IA-5(11)
IA-6	Authenticator Feedback	Contractor		
IA-7	Cryptographic Module Authentication	Contractor		
IA-8	Identification and Authentication (Non-Organizational Users)	Contractor		
IR-1	Incident Response Policy and Procedures	Shared		
IR-2	Incident Response Training	Shared		
IR-3	Incident Response Testing and Exercises	Contractor		IR-3(2) - Shared
IR-4	Incident Handling	Shared	A) Shared B) RCMP C) RCMP	IR-4(1)
IR-5	Incident Monitoring	Contractor		
IR-6	Incident Reporting	Contractor		IR-6(1)
IR-7	Incident Response Assistance	Contractor		IR-7(1) IR-7(2) - Shared
IR-8	Incident Response Plan	Contractor		
IR-9	Information Spillage Response	Shared	A) RCMP B) RCMP C) Shared D) Shared E) RCMP F) Shared	IR-9(1) IR-9(2) IR-9(3) - Shared IR-9(4) - Shared

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
MA-1	System Maintenance Policy and Procedures	Contractor		
MA-2	Controlled Maintenance	Shared	A) Contractor B) Shared C) Shared D) Contractor E) Contractor F) Contractor	MA-2(2)
MA-3	Maintenance Tools	Contractor		MA-3(1) MA-3(2) MA-3(3)
MA-4	Non-Local Maintenance	Shared	A) Shared B) Contractor C) Contractor D) Contractor	MA-4(1) MA-4(2) MA-4(3) MA-4(6) MA-4(7)
MA-5	Maintenance Personnel	Shared		MA-5(1)
MA-6	Timely Maintenance	Contractor		
MP-1	Media Protection Policy and Procedures	Contractor		
MP-2	Media Access	Contractor		
MP-3	Media Marking	Contractor		
MP-4	Media Storage	Contractor		
MP-5	Media Transport	Shared		MP-5(4)
MP-6	Media Sanitization	Contractor		MP-6(1) MP-6(2)

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
MP-7	Media Use	Contractor		MP-7(1)
PL-1	Security Planning Policy and Procedures	Contractor		
PL-2	System Security Plan	Shared		PL-2(3) - Shared
PL-4	Rules of Behaviour	Shared	Shared	PL-4(1)
PL-8	Information Security Architecture	Contractor		
PS-1	Personnel Security Policy and Procedures	Shared		
PS-2	Position Categorization	Shared		
PS-3	Personnel Screening	Shared		PS-3(3) - Shared
PS-4	Personnel Termination	Shared		PS-4(2) - Shared
PS-5	Personnel Transfer	Shared		
PS-6	Access Agreements	Shared		
PS-7	Third-Party Personnel Security	Shared		
PS-8	Personnel Sanctions	Shared		
RA-1	Risk Assessment Policy and Procedures	Shared		
RA-2	Security Categorization	Shared		
RA-3	Risk Assessment	Shared		
RA-5	Vulnerability Scanning	Contractor		RA-5(1) RA-5(2) RA-5(3) RA-5(5) RA-5(6) RA-5(8)

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
SA-1	System and Services Acquisition Policy and Procedures	Contractor		
SA-2	Allocation of Resources	Contractor		
SA-3	System Development Lifecycle	Contractor		
SA-4	Acquisition Process	Contractor		SA-4(1) SA-4(2) SA-4(3) SA-4(7) SA-4(8)
SA-5	Information System Documentation	Contractor		
SA-8	Security Engineering Principles	Contractor		
SA-9	External Information System Services	Contractor		SA-9(1) SA-9(2) SA-9(4) SA-9(5) (Data Residency)
SA-10	Developer Configuration Management	Contractor		SA-10(1)
SA-11	Developer Security Testing	Contractor		SA-11(1) SA-11(2) SA-11(8)
SA-12	Supply Chain Protection	Contractor		SA-12(1) SA-12(2) SA-12(5) SA-12(7) SA-12(8) SA-12(9) SA-12(11)

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
SA-14	Criticality Analysis	Contractor		
SA-15	Development Process, Standards, and Tool	Contractor		
SA-16	Developer Provided Training	Contractor		
SA-17	Developer Security Architecture and Design	Contractor		
SA-21	Developer Screening	Shared		
SC-1	System and Communications Protection Policy and Procedures	Contractor		
SC-2	Application Partitioning	Contractor		
SC-3	Security Function Isolation	Contractor		
SC-4	Information in Shared Resources	Contractor		
SC-5	Denial of Service Protection	Contractor		
SC-6	Resource Availability	Contractor		
SC-7	Boundary Protection	Shared		SC-7(3) SC-7(4) SC-7(5) SC-7(7) SC-7(8) SC-7(10) SC-7(12) SC-7(13) SC-7(14) SC-7(18) SC-7(19) SC-7(21) - Shared

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
SC-8	Transmission Confidentiality and Integrity	Shared		SC-8(1) - Shared
SC-10	Network Disconnect	Contractor		
SC-12	Cryptographic Key Establishment and Management	Shared		SC-12(2) - Shared SC-12(3) - Shared
SC-13	Cryptographic Protection	Contractor		
SC-15	Collaborative Computing Devices	Contractor		
SC-17	Public Key Infrastructure Certificates	Shared		
SC-18	Mobile Code	Shared	A) RCMP B) RCMP C) Contractor	SC-18(3) SC-18(4)
SC-19	Voice Over Internet Protocol	Shared	A) RCMP B) Contractor	
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	Contractor		
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	Contractor		
SC-22	Architecture and Provisioning for Name / Address Resolution Service	Contractor		
SC-23	Session Authenticity	Contractor		SC-23(1)
SC-28	Protection of Information At Rest	Contractor		SI-28(1)
SC-39	Process Isolation	Contractor		
SC-43	Usage Restrictions	Contractor		
SI-1	System and Information Integrity Policy and Procedures	Contractor		

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
SI-2	Flaw Remediation	Contractor		SI-2(1) SI-2(2) SI-2(3)
SI-3	Malicious Code Protection	Contractor		SI-3(1) SI-3(2) SI-3(7)
SI-4	Information System Monitoring	Contractor		SI-4(1) SI-4(2) SI-4(4) SI-4(5) SI-4(7) SI-4(11) SI-4(14) SI-4(16) SI-4(20) SI-4(22) SI-4(23)
SI-5	Security Alerts, Advisories, and Directives	Shared		SI-5(1)
SI-6	Security Functional Verification	Contractor		
SI-7	Software, Firmware, and Information Integrity	Contractor		SI-7(1) SI-7(5) SI-7(7)
SI-8	Spam Protection	Contractor		SI-8(1) SI-8(2)
SI-10	Information Input Validation	Contractor		

Table E-1: Security Requirements Traceability Matrix

Control ID	Control Name	NCS Control Responsibility	Responsibility for Multi-part Shared Control	Enhancements Assigned to Contractor
SI-11	Error Handling	Contractor		
SI-12	Information Output Handling and Retention	Contractor		
SI-15	Information Output Filtering	Contractor		
SI-16	Memory Protection	Contractor		

APPENDIX F – VOLUMETRICS

The following table contains NCS data volume estimates developed based on predicted Solution usage by Law Enforcement and Cybercrime Partners.

Table F-1: Year-Over-Year Estimated Data Growth

	Notes on Transaction Types	Estimated Transaction Volume (Yr)	Estimated Terabytes Yearly
A	Service Requests including queries, miscellaneous requests, requests for advice and guidance, knowledgebase access, ad hoc query requests, data submissions, coordination transactions, data preservation requests. Estimated 5 KB average transaction size.	725,000	3.4
B	Data Submissions - to Analyse and reply or just add to NC3 holdings. Each estimated at 500KB or less. (e.g. Cybercrime Investigations, Cybercrime Intelligence Analysis, Data Submissions to NC3 (Data Sharing))	15,000	0.007
C	5 GB Data Submissions. Approximately 1200 per year. Requests to Analyse and reply or just add to NC3 holdings. Size estimated at 5GB or less per submission.	1,200	5.9
D	Major Investigation Submissions (20 TB Each) - to Analyse and reply or just add to NC3 holdings. Major Investigation Submissions can be as large as 20TB – but can be substantially smaller or larger. Likely ingested using Large File Transfer or physical media. Scalability is key to handling these volumes.	5	97.6
E	Public Complaints include all cyber and fraud reports received via the NCFRS website. Most approximately 1KB data, however image attachments are accepted. Data estimate assumes 15% of submissions include an image of 250KB.	160,000	0.006
F	Includes miscellaneous threat and cybercrime intelligence feeds and special projects - estimated total 5 TB per year On a periodic basis the NCS will ingest miscellaneous data feeds related to cybercrime intelligence. These could be large data feeds containing "Web scrapes", MISP data or other threat intelligence data to be used for correlation and analysis. Data types and volumes vary; however large data sets are common. Source is Open Source and Private Cybercrime threat intelligence sources.	N.A.	4.9
		Total	**111.8**

The following table contains year-over-year estimated Transaction Volume growth.

Table F-2: Year-Over-Year Estimated Transaction Growth

Table F-1 Reference	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8
A	616250	688750	761250	797500	833750	841000	848250	855500
B	12750	14250	15750	16500	17250	17400	17550	17700
C	1020	1140	1260	1320	1380	1392	1404	1416
D	4	5	5	6	6	7	7	8
E	160,000	171,200	172,800	186,624	201,554	217,678	235,092	253,900

The following table contains year-over-year estimated projected growth of the NCS Data Repository and NCS User base.

Project Year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8
Total Terabytes accumulated Year over Year	103	230	377	537	710	890	1070	1250
Internal Users (Added)	170	150	100	20	20	20	20	20
External Users (Added)	200	700	600	75	75	75	75	75

APPENDIX G – CLOUD SERVICE DELIVERY MODEL REFERENCE TABLES

1. The Purpose of this appendix is to provide a framework for Contractors to provide references to detailed descriptions of their proposed Cloud Services and Resources (provided per System Architecture documentation in Section 4.1 – General Requirements) including:
    a. A table of all cloud infrastructure services and resources that the Contractor requires the RCMP to provision in order to operate and support the Contractor's Solution; and
    b. A table of all other proposed cloud services and resources.
2. Contractors proposing a Solution that will require the RCMP to provision Cloud Services and Resources (Where some or all of the Solution is hosted on the RCMP Cloud Tenant (IaaS or Private PaaS)) with the grant of perpetual licenses, must complete the applicable sections in Table G-1: Cloud Resources to be Provisioned by the RCMP. The following instructions apply:
    a. Indicate the Cloud Service Provider.
    b. Include brief description of each cloud service or resource that the RCMP will host on the RCMP's cloud tenant. Indicate a Page and Section Reference to the applicable details in the Contractor's CSDM Section of the proposed Solution Architecture.
    c. The Technical Authority requires all necessary detail to use a Cloud Service Provider Pricing Calculator to estimate costs of the cloud resources that the RCMP will be required to provision in order to support the proposed Solution.
    d. Use Cloud Service Provider (CSP) specific terminology to describe cloud services and resources including *types and sizes* that are applicable to the CSP.
    e. Provide a page/section reference to the System Architecture documentation (per Section 4.1 – General Requirements) that contains the details with respect to resource virtual instances, sizing, elasticity, scalability, high availability and resilience, 10 year data growth etc.
    f. Provide all details necessary for the RCMP to use a CSP price calculator to determine the cost of the cloud services or resources that the RCMP will host on the RCMP's cloud tenant.
2. Contractors proposing a Solution that involves use of SaaS or Public PaaS components must complete Table G-2: Solution Public PaaS and SaaS Cloud Resources.
    a. Include an indication of whether the service is qualified per SaaS-RFSA
    b. Include an indication of whether the service is approved per SSC GC Cloud Brokering Services for Protected B use
    c. Provide a page/section reference to the SaaS or Public PaaS component in the System Architecture for context and details with respect to how the Service addresses elasticity, scalability, resilience, 10-year data growth etc.

Table G-1: Cloud Resources to be Provisioned by the RCMP

Solution required RCMP Cloud Resources				
Cloud Service Provider:				
#	**Cloud Service Category**	**Brief Description of Service Names and Description**	**Reference to page and section of System Architecture CSDM**	**Architectural Component(s) being Addressed**
1	*Compute*	**Example:** *# of VM or EC2 Instances, High Availability, Region etc …* *Reference to CSP Service or Resource Part Number, SKU, etc*	*See Technical Proposal: System Architecture: CSDM Section 4.x.x*	*- Virtual Machines;* *- Compute Instances;* *- High Availability;*
	Data Storage			
	Network			
	Monitoring and Management			

Table G-1: Cloud Resources to be Provisioned by the RCMP

Solution required RCMP Cloud Resources				
Cloud Service Provider:				
#	**Cloud Service Category**	**Brief Description of Service Names and Description**	**Reference to page and section of System Architecture CSDM**	**Architectural Component(s) being Addressed**
	Other			

Table G-2: Solution Public PaaS and SaaS Cloud Resources

Public PaaS or SaaS Cloud Service Delivery Model Summary Table					
#	SaaS or Public PaaS Name and URL to SaaS Product	CSP Name	Reference to page and section of System Architecture - CSDM	SaaS-RFSA Tier 2 Qualified	SSC GC Cloud Brokering Protected-B Public Cloud Catalogue Approved

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915/C	-	155 XL
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
M7594-205915	155xl M7594-205915	

ANNEX B

BASIS OF PAYMENT

Bidders are required to use below Pricing Tables to submit their Financial Bid.

PRICING TABLE 1 (PT 1)		
PROTOTYPE SOLUTION (PS) FOR CAPABILITY AND USABILITY ASSESSMENT (CUA)		
Firm All-Inclusive Price in CAD (applicable taxes extra) for the Work described in Phase 1 - Prototype Solution of the Statement of Work in Annex A, including granting all Solution Usage Rights, Grants and Access, Software Documentation, Warranty, Virtual Training to use the Prototype, Maintenance and Support, Waivers, Non-disclosure Agreements and any other releases to Canada for purposes of conducting the CUA assessment, for up to 100 to use the PS for CUA purposes during the initial contract period.		
Item # (A)	**Description (B)**	**Firm All-Inclusive Lot Price (C)**
1	All deliverables associated with Phase 1, including the Prototype Solution in accordance with Annex A – Statement of Work.	200 000 $
PT1: Total Evaluated Bid Price (Sum of (C))		**200 000 $**

PRICING TABLE 2 (PT2)		
PROTOTYPE ON PLATFORM (PoP) TESTING (if applicable)		
Firm All-Inclusive Price in CAD (applicable taxes extra) for proof of a successful installation and deployment of the Contractor's Prototype Solution, if applicable, in accordance with the Contractor's Protected B Cloud Deployment Model defined per Annex A- Statement of Work including but not limited to, granting all Solution usage rights, grants and access, Software Documentation, Warranty, Maintenance and Support (excluding Training), waivers, non-disclosure agreements and any other releases to Canada for purposes of conducting the PoP Test, for up to 100 Users to use the Prototype Solution for test validation purposes.		
Item # (A)	**Description (B)**	**Firm All-Inclusive Lot Price (C)**
1	Successful completion of PoP Test in accordance with Annex A – Statement of Work.	25 000 $
PT2: Total Evaluated Bid Price (Sum of (C))		**25 000 $**
Note: POP Test may be applicable, at Canada's sole discretion.		

INSTRUCTIONS TO BIDDERS FOR TABLE 3
Bidders are required to complete the Implementation of Solution Table for their solution aligning with the Implementation Plan as per Annex A – Statement of Work.

PRICING TABLE 3 (PT3)		
IMPLEMENTATION OF SOLUTION		
Firm All-Inclusive Price in CAD (applicable taxes extra) for the delivery of the Full Solution (regardless the model purposed: on premise, hybrid or SaaS) with the functionality as described in the Annex A – Statement of Work. Includes Solution Planning, implementation support (if applicable), integration support (if applicable), configuration, training, updated training material, creation and upkeep of on-line training, warranty (if applicable), waivers, non-disclosure agreements and other releases to Canada.		
Item # (A)	**Description (B)**	**Firm All-Inclusive Lot Price (C)**
1	Delivery of the NCS solution	$_____
PT3: Total Evaluated Bid Price (Sum of (C))		**$**

INSTRUCTIONS TO BIDDERS FOR TABLE 4
Bidders are required to provide prices for all appropriate line items that align with their Solution delivery model and as per Annex A-Statement of work (SOW). If their Solution involves, both, Perpetual License AND User Access approaches, the bidder is requested to add prices in both lines (#a and #b). If just one line item (approach) is required, namely #a or #b, the bidder is required to add 0.00 to each line item where price is not required.

PRICING TABLE 4 (PT4)				
GRANT FOR ADDITIONAL USER LICENSES (if applicable) OR USER ACCESSES (if applicable) OR USER LICENSES and USER ACCESSES (if applicable) DURING IMPLEMENTATION PERIOD				
Firm All-Inclusive Price in CAD (applicable taxes extra)				
Item #a - #b (A)	**Description (B)**	**Price per User (C)**	**Number of Users (D)**	**Extended Price for Evaluation Purpose (E) = ((C) X (D))**
1a	User Licenses as per Annex A-SOW	$_____	100	$_____
1b	User Accesses as per Annex A-SOW	$_____	100	$_____
PT4: Total Evaluated Bid Price (Sum of prices under (E))				$_____
Note: For evaluation purpose, 100 is the estimated number of users by period.				

INSTRUCTIONS TO BIDDERS FOR TABLE 5A AND 5B
Bidders are required to provide prices for all appropriate line items that align with their Solution delivery model and as per Annex A-Statement of work (SOW). If their Solution involves, both, User License AND User Access approaches, the bidder is requested to add prices in both tables (PT5A and PT5B). If just one Table (approach) is required, namely PT5A or PT5B, the bidder is required to add 0.00 to each line item of Table where price is not required.

PRICING TABLE 5A (PT5A)				
OPTIONAL GRANT PER ADDITIONAL USER LICENSE (if applicable)				
Firm All-Inclusive Price in CAD (applicable taxes extra)				
Item (A)	**Description (B)**	**Price per Additional User (C)**	**Additional Users (D)**	**Extended Price for Evaluation Purpose (E) = ((C) X (D))**
1	Option Year 1: Additional User Licenses as per Annex A-SOW	$_____	100	$_____
2	Option Year 2: Additional User Licenses as per Annex A-SOW	$_____	100	$_____
3	Option Year 3: Additional User Licenses as per Annex A-SOW	$_____	100	$_____
4	Option Year 4: Additional User Licenses as per Annex A-SOW	$_____	100	$_____
5	Option Year 5: Additional User Licenses as per Annex A-SOW	$_____	100	$_____
6	Option Year 6: Additional User Licenses as per Annex A-SOW	$_____	100	$_____
7	Option Year 7: Additional User Licenses as per Annex A-SOW	$_____	100	$_____
8	Option Year 8: Additional User Licenses as per Annex A-SOW	$_____	100	$_____
PT5A: Total Evaluated Bid Price (Sum of prices under (E) ÷ 8)				$_____
Note: For evaluation purpose, 100 is the estimated number of additional users by period.				

PRICING TABLE 5B (PT5B)										
OPTIONAL GRANT FOR ADDITIONAL USER ACCESS (if applicable)										
Firm All-Inclusive Price in CAD (applicable taxes extra) for Additional User Access to Hosted Solution capable of processing the described Transaction Volumes										
Item #	**Processing Transaction Volume**	**Firm All-Inclusive Price per Transaction Volume Lot for <u>100 Additional User Accesses</u> per Optional Period (OP)**								**Extended Price for Evaluation Purpose**
		OP 1	**OP 2**	**OP 3**	**OP 4**	**OP 5**	**OP 6**	**OP 7**	**OP 8**	
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**	**(G)**	**(H)**	**(I)**	**(J)**	**Σ(C,…,J) (L)**
1	1 to 250,000	$___	$___	$___	$___	$___	$___	$___	$___	$_____
2	250,001 to 500,000	$___	$___	$___	$___	$___	$___	$___	$___	$_____
3	500,001 to 750,000	$___	$___	$___	$___	$___	$___	$___	$___	$_____
4	750,001 to 1,000,000	$___	$___	$___	$___	$___	$___	$___	$___	$_____
5	1,000,001 to 1,250,000	$___	$___	$___	$___	$___	$___	$___	$___	$_____
6	More than 1,250,000	$___	$___	$___	$___	$___	$___	$___	$___	$_____
PT5B: Total Evaluated Bid Price (Sum of prices under (L) ÷ 8))										$_____
Note: For evaluation purpose, 100 is the estimated number of additional users by period.										

INSTRUCTIONS TO BIDDERS FOR TABLE 6
Bidders are required to provide prices for all appropriate line items that align with their Solution delivery model. If their Solution involves, both, Solution Maintenance and Support Services AND Hosting and Hosting Related Support Services, the bidder is requested to add prices in both lines (#a and #b). If just one line item set being required , namely #a or #b, the bidder is required to add 0.00 to each line item where price is not required.

PRICING TABLE 6 (PT6)			
OPTIONAL SOLUTION MAINTENANCE AND SUPPORT SERVICES (if applicable) OR NCS HOSTING AND HOSTING RELATED SUPPORT SERVICES (if applicable) OR SOLUTION MAINTENANCE AND SUPPORT SERVICES and NCS HOSTING AND HOSTING RELATED SUPPORT SERVICES (if applicable)			
Firm All-Inclusive Price in CAD (applicable taxes extra)			
Item #a - #b (A)	**Description** For the provision of NCS Maintenance and Support services or NCS Hosting and Hosting Related Support Services or for Combination of previous Service Sets during Option Period (OP), as applicable. **(B)**	**Lot Price (C)**	**Total Price per Period (#a + #b) (D)**
1a	OP 1: Solution Maintenance and Support Services	$_____	$_____
1b	OP 1: NCS Hosting and Hosting Related Support Services	$_____	
2a	OP 2: Solution Maintenance and Support Services	$_____	$_____
2b	OP 2: NCS Hosting and Hosting Related Support Services	$_____	
3a	OP 3: Solution Maintenance and Support Services	$_____	$_____
3b	OP 3: NCS Hosting and Hosting Related Support Services	$_____	
4a	OP 4: Solution Maintenance and Support Services	$_____	$_____
4b	OP 4: NCS Hosting and Hosting Related Support Services	$_____	
5a	OP 5: Solution Maintenance and Support Services	$_____	$_____
5b	OP 5: NCS Hosting and Hosting Related Support Services	$_____	
6a	OP 6: Solution Maintenance and Support Services	$_____	$_____
6b	OP 6: NCS Hosting and Hosting Related Support Services	$_____	
7a	OP 7: Solution Maintenance and Support Services	$_____	$_____
7b	OP 7: NCS Hosting and Hosting Related Support Services	$_____	
8a	OP 8: Solution Maintenance and Support Services	$_____	$_____
8b	OP 8: NCS Hosting and Hosting Related Support Services	$_____	
PT6: Total Evaluated Bid Price (Sum of all prices under (D))			$_____

INSTRUCTIONS TO BIDDERS FOR TABLE 7
Bidders are required to indicate **all** professional service categories (B) required, with per diem (C-J) and average extended prices (K) for their solution during each optional periods.

PRICING TABLE 7 (PT7)

OPTIONAL PROFESSIONAL SERVICES

Firm All-Inclusive Price in CAD (applicable taxes extra) per diem rates for Optional Professional Services (PS) to be provided on an as-and-when requested basis as described in Annex A – Statement of Work and in accordance with the Task Authorization process

Item #	PS Category Description	Per Diem Firm All-Inclusive Price per Optional Period (OP)								Average Extended Price per Period per PS: Σ(C,D,…,J) X 100 ÷ 8
		OP 1 per diem	OP 2 per diem	OP 3 per diem	OP 4 per diem	OP 5 per diem	OP 6 per diem	OP 7 per diem	OP 8 per diem	
(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)
1										
2										
3										
4										
5										
PT7: Total Evaluated Bid Price (Sum of all prices (K) ÷ (Total number of categories))										

Notes: For evaluation purposes, 100 represents the estimated Level of Effort in days for each category and period. A Total Evaluated Bid Price averaged on the number of categories allows a bidder to provide any number of foreseeable PS categories required during Option Periods without being disadvantaged in the course of the Financial Evaluation.

INSTRUCTIONS TO BIDDERS FOR TABLE 8
Bidders are required to complete the below table and add any additional required training categories (B), and indicate per trainee prices (C-J) and per trainee price averages (K) by category for their solution during option periods.

PRICING TABLE 8 (PT8)

OPTIONAL TRAINING SERVICES

Firm All-Inclusive Price in CAD (applicable taxes extra) per user for training for virtual Training Services on an as-and-when requested basis, as detailed in Annex A – Statement of Work
and in accordance with the Task Authorization process

Item #	Training Category Description	Firm All-Inclusive Price per Trainee during Optional Period (OP)								Average Extended Price per Period for 100 Trainees: Σ(C,D,…,J) X 100 ÷ 8
		OP 1	OP 2	OP 3	OP 4	OP 5	OP 6	OP 7	OP 8	
(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)
1	End-User									
2	Power User									
3	SME User									
4	Technical Support User									
5										
6										
PT8: Total Evaluated Bid Price (Sum of all prices (K) ÷ (Total number of categories))										

Notes: For evaluation purposes, 100 represents the estimated number of trainees for each option period. A Total Evaluated Bid Price averaged on the number of categories allows a bidder to provide any foreseeable training categories required during option periods without being disadvantaged in the course of the Financial Evaluation.

Total Evaluated Bid Price to compute the Financial Score = Σ (PT1, PT2, …, PT8)

TABLE SCHEDULE OF MILESTONE PAYMENTS		
IMPLEMENTATION SUPPORT		
Item # (A)	**Description (B)**	**All-Inclusive Lot Price (C)**
1	Milestone #1 • Per agreed implementation timeline • Accepted BCM Functionality (As per agreed Implementation Plan)	5%
2	Milestone #2 • Per agreed implementation timeline • Accepted BCM Functionality (As per agreed Implementation Plan)	10%
3	Milestone #3 • Per agreed implementation timeline • Accepted BCM Functionality (As per agreed Implementation Plan)	10%
4	Milestone #4 • Per agreed implementation timeline • Accepted BCM Functionality (As per agreed Implementation Plan)	10%
5	Milestone #5 • Per agreed implementation timeline • Accepted BCM Functionality (As per agreed Implementation Plan)	10%
6	Milestone #6 • Per agreed implementation timeline • Accepted BCM Functionality (As per agreed Implementation Plan)	20%
7	Milestone #7 • Per agreed implementation timeline • Accepted Delivery of Final Operating Capability Solution	35%
Total implementation price in percentage		100%
Note: These percentage are determined by Canada, at its sole discretion.		

ANNEX C

SECURITY REQUIREMENT CHECK LIST – PHASE 1 - PROTOTYPE

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915	-	155 XL
Client Ref. No. - N° de réf. du client	**File No. - N° du dossier**	**CCC No./N° CCC - FMS No./N° VME**
M7594-205915	155xl M7594-205915	

Government of Canada / Gouvernement du Canada

SRCL# 20201119075 - PROTOTYPE

Contract Number / Numéro du contrat
202005915 / M7594-205915
Security Classification / Classification de sécurité
PROTECTED A

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
RCMP	IM/IT - NHQ / CIO / SDPPM

3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

The work to be performed is for the prototyping of a National Cybercrime IM/IT Solution. An agile procurement process will be used, which includes the award of (3) prototype contracts to (3) different vendors, prior to issuance of the contract for the final solution. The prototype contracts will enable to assess the functionality of solution that is being proposed by the 3 vendors. Vendors' personnel will not require access to ROSS or to RCMP data during the prototype phase.

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

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

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☑ No / Non	☐ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☐ No / Non	☑ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

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

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

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

PROTECTED A / PROTÉGÉ A ☐	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☐	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

SRCL# 20201119075 - PROTOTYPE

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915 / M7594-205915
Security Classification / Classification de sécurité
PROTECTED A

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

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

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

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

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

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

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

Special comments:
Commentaires spéciaux : ON SITE - Facility Access II with escort - Accès aux installations II avec escorte
OFF SITE - Facility Access II without escort - Accès aux installations II sans escorte

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

SRCL# 20201119075 - PROTOTYPE

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202005915 / M7594-205915
Security Classification / Classification de sécurité
PROTECTED A

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

☐ No / Non ☑ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Government of Canada / Gouvernement du Canada

SRCL# 20201119075 - PROTOTYPE

Contract Number / Numéro du contrat
202005915/ M7594-205915
Security Classification / Classification de sécurité
PROTECTED A

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	
Dusan Musal	Director	Dusan Musal Digitally signed by Musal,Dusan,000169308 Date: 2020.04.27 12:02:20 -04'00'	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613-998-7329		Dusan.Musal@rcmp-grc.gc.ca	2020/04/27

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sheila Nordskog	Security Analyst		
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
613-843-5247	613-823-0143	sheila.nordskog@rcmp-grc.gc.ca	2020-07-29

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	
Mary Rutledge	A/Manager - Procurement Special Projects	Mary Rutledge	
Telephone No. - N° de téléphone	**Facsimile No. - N° de télécopieur**	**E-mail address - Adresse courriel**	**Date**
343-552-2386 / 613-843-6935		mary.rutledge@rcmp-grc.gc.ca	2020/05/15

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**

SRCL Security Guide – NCS Prototype

SRCL Security Guide

National Cybercrime Solution - Prototype
SRCL #: 20201119075

Prepared by :
Central Departmental Security Section
Royal Canadian Mounted Police

General Security Requirements

All contractors employed on this contract must support the RCMP's security environment by complying with the directives described in this document.

1. All Protected information (hard copy documentation) or other sensitive assets for which the RCMP is responsible will be shared with the contractor through pre-approved processes.

2. The information disclosed by the RCMP will be administered, maintained, and disposed of in accordance with the Contract. At minimum the contractor must follow the Policy on Government Security.

3. The contractor will promptly notify the RCMP of any unauthorized use or disclosure of the information exchanged under this contract and will furnish the RCMP with details of the unauthorized use or disclosure. (i.e. loss of sensitive information, accidental or deliberate.)

4. Photography is not permitted. If photos are required, please contact the Organization Project Authority and Departmental Security Section.

5. The use of personal property, e.g. desktop peripherals, communication devices, portable storage media such as USB sticks, in conjunction with RCMP technology is prohibited

6. The contractor is not permitted to disclose sensitive information provided by the RCMP, to any sub-contractors, without those individuals having the proper RCMP security level required to access the protected information.

7. The RCMP's Departmental Security Section (DSS) reserves the right to:
    - conduct inspections of the contractor's site/premises. Inspections may be performed prior to sensitive information being shared and/or as required (i.e. if the contractor's work location relocates). The intent of the inspection is to ensure the quality of security safeguards.
    - request photographic verification of the security safeguards. Photographs may be requested prior to sensitive information being shared and/or as required (i.e. if the contractor's work location relocates). The intent of the photographs is to ensure the quality of security safeguards.
    - provide guidance on mandatory safeguards (safeguards as specified in this document and possibly additional site specific safeguards).

8. To ensure Canada's sovereign control over its data, all sensitive or protected data under government control will be stored on servers that reside in Canada. Data in transit will be appropriately encrypted.

Physical Security

1. No Protected A or B information (hard copy documentation (i.e. notes)) or other assets will be removed from the RCMP facility without the approval of the Departmental representative. If approved, the transport, transmittal, storage, and destruction must comply with the security requirements identified in the RCMP's Security Manuals.

2. Only sanitized drawings will be physically present at the contractor's location (i.e. no Protected or Classified information will be present). To properly sanitize floor plans, the contractor must ensure that the drawings meet the following requirements;

   - Construction drawings will not contain a key plan showing the entire complex or site.
   - RCMP logos, RCMP name, or site address will not be shown on the construction drawings.
   - PWGSC or Government of Canada identifiers will be used
   - Rooms must be identified by number, not names. A separate coded list of room numbers associated to sensitive information and descriptors will be developed and updated as changes are made.
   - Security system information will be placed on separate layers of construction drawings for ease of printing and distribution.

IT Security

1. No sensitive information, Protected A or higher, shall be electronically transmitted outside of RCMP networks or processed at the contractor's site.

2. No sensitive electronic information or assets, Protected A or higher, shall be removed from RCMP networks or property.
3. The use of personal property, e.g. desktop peripherals, communication devices, portable storage media such as USB sticks, in conjunction with RCMP technology is prohibited.

4. Individuals must not use privately-owned technology to join, bridge, or participate with RCMP networks in any way on RCMP premises including creating a network or access point

5. Only contractors who have a RCMP ERS security clearance are permitted to use a personal cell phone (with prior permission) on RCMP premises, however communication;
    a. must be restricted to non-sensitive information;
    b. must not be used to conduct RCMP business and;
    c. must not be connected to RCMP communications technology at any time.

6. Do not store Protected A/B information, encrypted or not, on systems, networks, or storage media, unless they are specifically approved for that purpose

Personnel Security

1. Contractor and sub-contractor personnel will be required to obtain and maintain a RCMP personnel security clearance/status commensurate with the sensitivity of the work being performed throughout the life cycle of the contract (in accordance with the provisions of the SRCL).

2. The contractor will be responsible for advising the RCMP of any changes in personnel security requirements. For example: Cleared personnel leaving the company or no longer supporting the RCMP contract, new personnel requiring security screening and personnel requiring renewal of their personnel security screening.

Facility Access Level II: When the supplier and its employees will only require access to a RCMP Facility or site and will not have access to protected or classified information, systems or assets, an RCMP Clearance at the appropriate level is required. Contractor personnel must submit to local law enforcement verification by the RCMP, prior to being granted access to facility or site. The RCMP reserves the right to deny access to any of the contractor personnel, at any time.

When the RCMP requires **Facility Access Level II**; the successful Bidder, Contractor will submit the following to the RCMP:

- Form TBS 330-23 (LERC Version)
- Copy of Government Issued Photo Identification (Driver's License Front and Back)

The RCMP:

- Will conduct personnel security screening checks above the Policy on Government Security requirements.
- Is responsible for escort requirements on its facilities or sites.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915	-	155 XL
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
M7594-205915	155xl M7594-205915	

SECURITY REQUIREMENTS CHECKLIST – PHASE II – FULL SOLUTION

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
M7594-205915	-	155 XL
Client Ref. No. - N° de réf. du client	**File No. - N° du dossier**	**CCC No./N° CCC - FMS No./N° VME**
M7594-205915	155xl M7594-205915	

Government of Canada / Gouvernement du Canada

AMENDED SRCL# 202011119075 - FINAL SOLUTION

Contract Number / Numéro du contrat
202005915
Security Classification / Classification de sécurité
PROTECTED A

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
RCMP	IM/IT - NHQ / CIO / SDPPM

3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

The work to be performed includes design, architecture, configuration and implementation of the final National Cybercrime IM/IT Solution. An agile procurement process will be used. The work to be done will be performed by one of the (3) prototype vendors after issuance of the contract for the final solution. The final solution vendor will require access to RCMP facilities and may require access to ROSS and RCMP data.

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 / OTAN		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)	☐

Government of Canada / Gouvernement du Canada

SRCL# 202011119075 - FINAL SOLUTION

Contract Number / Numéro du contrat
202005915
Security Classification / Classification de sécurité
PROTECTED A

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

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

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

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

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

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

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

Special comments:
Commentaires spéciaux :

Between prototype and the POP Test phase the FA2 resource will be subject to following restrictions until receiving the ERS(non-privileged access) or ERS+SECRET(privileged access):
- The FA2 resource cannot receive any RCMP login credentials;
- The FA2 resource must be escorted by an appropriately cleared individual; and
- The FA2 resource may guide an appropriately cleared individual who will have hands on keyboard.

For the Pop Test & Final Solution: Once the security levels are finalized and the list of resources to clear for the identified roles is received, the security clearance process will start during the POP test Phase.

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

SRCL# 202011119075 - FINAL SOLUTION

Contract Number / Numéro du contrat
202005915
Security Classification / Classification de sécurité
PROTECTED A

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

☐ No / Non ☑ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Government of Canada / Gouvernement du Canada

SRCL# 202011119075 - FINAL SOLUTION

Contract Number / Numéro du contrat
202005915
Security Classification / Classification de sécurité
PROTECTED A

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	
Dusan Musal	Director, NC3 Project	Digitally signed by Musal,Dusan,000169308 Date: 2020.04.27 12:03:16 -04'00'	
Telephone No. - N° de téléphone: 613-998-7329	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel: dusan.musal@rcmp-grc.gc.ca	Date: 2020/04/27

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sheila Nordskog	Security Analyst	SRCL AMENDED 2020-10-06 SNORDSKOG	
Telephone No. - N° de téléphone: 613-843-5247	Facsimile No. - N° de télécopieur: 613-823-0143	E-mail address - Adresse courriel: sheila.nordskog@rcmp-grc.gc.ca	Date: 2020-07-29

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	
Mary Rutledge	A/Manager- Procurement Special Projects	Mary Rutledge	
Telephone No. - N° de téléphone: 343-552-2386 / 613-843-6935	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel: mary.rutledge@rcmp-grc.gc.ca	Date: 2020/05/15

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

SRCL Security Guide

National Cybercrime Solution – Final Solution
SRCL #: 20201119075

Prepared by:
Central Departmental Security Section
Royal Canadian Mounted Police

General Security Requirements

All contractors employed on this contract must support the RCMP's security environment by complying with the directives described in this document.

9. All Protected information (hard copy documentation) or other sensitive assets for which the RCMP is responsible will be shared with the contractor through pre-approved processes.

10. The information disclosed by the RCMP will be administered, maintained, and disposed of in accordance with the Contract. At minimum the contractor must follow the Policy on Government Security.

11. The contractor will promptly notify the RCMP of any unauthorized use or disclosure of the information exchanged under this contract and will furnish the RCMP with details of the unauthorized use or disclosure. (i.e. loss of sensitive information, accidental or deliberate.)

12. Photography is not permitted. If photos are required, please contact the Organization Project Authority and Departmental Security Section.

13. The use of personal property, e.g. desktop peripherals, communication devices, portable storage media such as USB sticks, in conjunction with RCMP technology is prohibited

14. The contractor is not permitted to disclose sensitive information provided by the RCMP, to any sub-contractors, without those individuals having the proper RCMP security level required to access the protected information.

15. The RCMP's Departmental Security Section (DSS) reserves the right to:
    - conduct inspections of the contractor's site/premises. Inspections may be performed prior to sensitive information being shared and/or as required (i.e. if the contractor's work location relocates). The intent of the inspection is to ensure the quality of security safeguards.
    - request photographic verification of the security safeguards. Photographs may be requested prior to sensitive information being shared and/or as required (i.e. if the contractor's work location relocates). The intent of the photographs is to ensure the quality of security safeguards.
    - provide guidance on mandatory safeguards (safeguards as specified in this document and possibly additional site specific safeguards).

16. To ensure Canada's sovereign control over its data, all sensitive or protected data under government control will be stored on servers that reside in Canada. Data in transit will be appropriately encrypted.

Physical Security

The Physical Security measures below are contingent on and subordinate to the appropriate permission being granted within the SRCL.

1. **Storage**: Protected information/assets must be stored in a container acceptable to the RCMP DSS. The container must be located (at minimum) within an "Operations Zone". As such, the contractor's facility must have an area/room that meets the following criteria:

Operations Zone	
Definition	An area where access is limited to personnel who work there and to properly escorted visitors. Note: The personnel working within the Operational Zone must: • possess a valid RCMP Reliability Status (RRS), or • be escorted by an individual who possesses a valid RRS
Perimeter	Must be indicated by a recognizable perimeter or a secure perimeter depending on project needs. For example, the controls may be a locked office or suite.
Monitoring	Monitored periodically by authorized employees. For example, users of the space working at the location are able to observe if there has been a breach of security.

Note: Refer to Appendix A for more information on the Security Zone concept.

2. **Discussions**: Where sensitive conversations are anticipated, Operations Zones must have a stand off from public spaces or be designed with acoustic speech privacy properties (where the user has a reasonable expectation that they will not be overheard). For example, private room/office and/or boardroom.

3. **Production**: The production (generation and/or modification) of Protected information or assets must occur in an area that meets the criteria of an Operations Zone.

4. **Destruction**: All drafts or misprints (damaged copies and/or left over copies) must be destroyed by the contractor. Protected information must be destroyed in accordance with the RCMP's Security Manual. The equipment/system (i.e. shredder) used to destroy sensitive material is rated according to the degree of destruction. RCMP approved destruction equipment must be utilized.

   Approved levels of destruction for Protected B include:

   - Residue size must be less than 1 x 14.3 mm (particle cut).

   Note:

- If the contractor is unable to meet the RCMP's destruction requirements, all sensitive information/assets are to be returned to the RCMP for proper destruction.
- Any sensitive drafts/misprints awaiting disposal must be protected in the agreed upon manner until destroyed.

5. **Transport/Transmittal:** The physical exchange of sensitive information must follow the Contract. When a delivery service is used, it must offer proof of mailing, a record while in transit and of delivery.

Transport	Transport: to transfer sensitive information and assets from one person or place to another by someone with a need to know the information or need to access the asset.
Transmittal	Transmit: to transfer sensitive information and assets from one person or place to another by someone without a need to know the information or need to access the asset.

Note:

- For Transport of Protected "B" information (travel to/from neutral locations for meetings and/or interviews): In place of a single envelope, a briefcase or other container of equal or greater strength may be used. Double envelope/wrap to protect fragile contents or to keep bulky, heavy or large parcels intact.
- For Transmittal of Protected "B" information (Canada Post or registered courier): Address in a nonspecific manner. Add "To Be Opened Only By" because of the need-to-know or need-to-access principles when warranted.

IT Security

Appropriate Control of Protected A and B Information

Transport/Transmittal

1. Protected A/B information must not be released into the public domain.

2. The use of personal property, e.g. desktop peripherals, communication devices, portable storage media such as USB sticks, in conjunction with RCMP technology is prohibited.

3. Contractors must not use privately-owned technology to join, bridge, or participate with RCMP networks in any way on RCMP premises including creating a network or access point.

4. Contractors can transmit Protected A information, i.e. voice and data, over any network under the stewardship of the RCMP and associated RCMP-approved infrastructure, without using additional safeguards, e.g. without encryption.

5. Contractors can process Protected-B information locally on ROSS workstation computers, but must encrypt Protected-B information with the corporate standard encryption solution to store or transmit it.

6. Contractors must use an RCMP-approved encryption solution or application rated for Protected-B when Protected-B information is transmitted both internally, i.e. networks under the stewardship of the RCMP, and externally.

Telephony

1. Contractors may use standard RCMP office telephones to communicate Protected A information.

   NOTE: Office telephone means a telephone intended to be used at an individual's desk, rather than a mobile or cellular phone.

2. Individuals must not use standard office telephones for Protected-B information.

3. All voice communication by any cellular, mobile or land line telephone must be restricted to non-sensitive information, unless the phone is specifically accredited and issued for sensitive information.

4. Only contractors who have a RCMP ERS security clearance are permitted to use a personal cell phone (with prior permission) on RCMP premises, however communication;
   - must be restricted to non-sensitive information;
   - must not be used to conduct RCMP business and;
   - must not be connected to RCMP communications technology at any time.

Printing, Scanning, and Photocopying

1. Printing, scanning, or copying of Protected A/B information is only permitted using RCMP issued equipment.

Storing

1. Do not store Protected A/B information, encrypted or not, on systems, networks, or storage media, unless they are specifically approved for that purpose.

2. Individuals must safeguard Protected-B information when stored, i.e. when not in use, by:
   - encrypting the Protected-B information using an RCMP-approved encryption solution, and storing it using local ROSS system storage/ROSS network resources;
   - using an application rated for Protected-B;

- using authorized physical security safeguards;

3. PKI tokens, identity cards, building access cards, and other objects used to log in to applications, systems, and other technology, or encrypt, decrypt, digitally sign, or securely delete, must never be left unattended in proximity of the technology with which they are used.

4. All RCMP supplied storage devices used throughout the duration of this contract must be returned to the RCMP immediately upon contract termination.

Personnel Security

1. All contractor and sub-contractor personnel will be required to obtain and maintain a personnel security clearance/status commensurate with the sensitivity of the work being performed throughout the life cycle of the contract (in accordance with the provisions of the SRCL).

2. The contractor will be responsible for advising the RCMP of any changes in personnel security requirements. For example: Cleared personnel leaving the company or no longer supporting the RCMP contract, new personnel requiring security screening and personnel requiring renewal of their personnel security screening.

3. As the supplier and its employees will have access to RCMP Protected and/or Classified information, an RCMP Clearance at the appropriate level is required.
   Contractor personnel must submit to verification by the RCMP, prior to being granted access to Protected or Classified information, systems, assets and/or facilities. The RCMP reserves the right to deny access to any of the contractor personnel, at any time.

   When the RCMP identifies a requirement for ERS or a security clearance; the Contractor will submit the following to the RCMP:

1. Form TBS 330-23 (LERC version)
2. Form TBS 330-60
3. Form RCMP 1020-1 (Pre Interview)
4. Copy of Birth Certificate and Driver's License
5. 2 Passport size pictures.

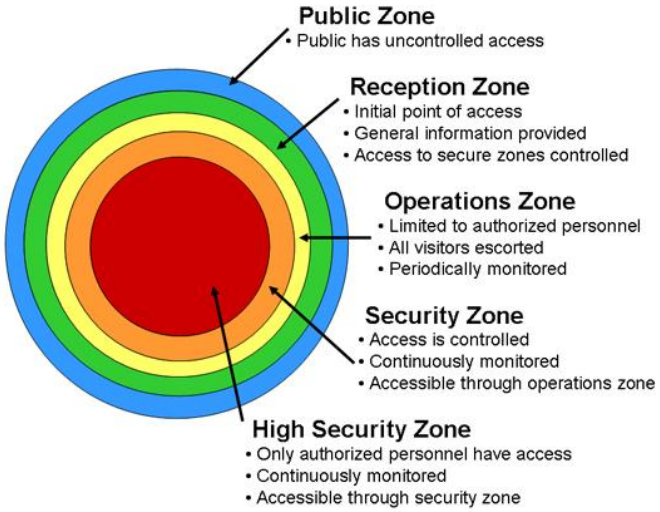
The RCMP:

1. will conduct personnel security screening checks above and beyond the security requirements outlined in the *Policy on Government Security*
2. will conduct a security interview
3. will obtain a set of fingerprints

Appendix A – Security Zone Concept

The *Government Security Policy (Section 10.8 - Access Limitations)* stipulates that "departments must limit access to classified and protected information and other assets to those individuals who have a need to know the information and who have the appropriate security screening level".

The *Operational Security Standard on Physical Security (Section 6.2 - Hierarchy of Zones)* states that "departments must ensure that access to and safeguards for protected and classified assets are based on a clearly discernable hierarchy of zones".



Public Zone is where the public has unimpeded access and generally surrounds or forms part of a government facility. Examples: the grounds surrounding a building, or public corridors and elevator lobbies in multiple occupancy buildings.

Reception Zone is where the transition from a public zone to a restricted-access area is demarcated and controlled. It is typically located at the entry to the facility where initial contact between visitors and the department occurs; this can include such spaces as places where services are provided and information is exchanged. Access by visitors may be limited to specific times of the day or for specific reasons.

Operations Zone is an area where access is limited to personnel who work there and to properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored periodically. Examples: typical open office space, or typical electrical room.

Security Zone is an area to which access is limited to authorized personnel and to authorized and properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously, i.e., 24 hours a day and 7 days a week. Example: an area where secret information is processed or stored.

High Security Zone is an area to which access is limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors; it must be indicated by a perimeter built to the specifications recommended in the TRA, monitored continuously, i.e., 24 hours a day and 7 days a week and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel.

Access to the zones should be based on the concept of "need to know" and restricting access to protect employees and valuable assets. Refer to RCMP Guide G1-026, Guide to the Application of Physical Security Zones for more detailed information.

APPENDIX A TO ANNEX C –

SECURITY CLASSIFICATION GUIDE

The following table outlines the personnel and facility security clearance requirements based on the expected roles and access to GC data.

Table A-1 Security Classification Guide for Commercial Cloud Services

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Responsibility	Details
1.	Any Contractor personnel with physical access to the Contractor data centers	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local Backup Media	Canada	Reliability	Contractor	This is for any Contractor personnel including facilities management resources that have physical access to the Cloud Services hardware equipment at the Contractor data centers.
2.	Any Contractor personnel who have logical access to the Contractor services	• All Business Data • Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components	Both	Reliability	Contractor	This is for any Contractor personnel that has logical access to the GC data hosted in the Contractor data centers and any sensitive system and security incident data.
3.	Any Contractor personnel with privileged roles and unrestricted logical access to GC assets within the Contractor services	• All Business Data • GC Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components • Assets include GC data and credentials	Both	Secret	Contractor	This is for any Contractor personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the Contractor data centers and any sensitive system and security incident data. This includes authorized access through an established process such as legal requests.

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Responsibility	Details
4.	Any Contractor personnel or Reseller who has access to the GC Master Account information and/or credentials	• GC Master Account Information/Credentials	Both	Reliability	Contractor and/or Reseller	This is for any Contractor or Reseller personnel that has access to the GC master account or root credentials for the cloud service account setup.
5.	Prime Contractor*	Media	Both	Reliability	Contractor	Information that is sent from Prime Contractor to Subcontractor - needs to be encrypted.
6.	Operations Manager/Personnel *	Name, addresses, email, phone numbers and data centers	Both	Reliability	Contractor	Information that is sent from Prime Contractor to Subcontractor - needs to be encrypted.
7.	General duties	Public and reception zones	Both	N/A	Contractor	
8.	General duties*	Sensitive sites (such as operational zones where data is stored)	Both	Reliability Status	Contractor	*Information within site may be of sensitive nature. Individuals who are not screened must be escorted at all times. General duties include personnel providing maintenance services, security guards in the Operational Zone, etc.

*The Contractor must contact PSPC CISD to ensure that the appropriate sub-SRCL is established for Sub-Contractors.

APPENDIX B TO ANNEX C –

SECURITY OBLIGATIONS

Security Obligations

The obligations of the Contractor contained in these Security Obligations must be flowed down by the Contractor to Sub-processors, to the extent applicable to each Contractor Sub-processor, given the nature of the Public Cloud Services provided by it to the Contractor.

1. Change Management.

(a) The Contractor must, throughout the Contract, take all steps required to update and maintain the Security Obligations as needed to comply with the security practices of industry standards.

(b) The Contractor must advise Canada of all improvements that affect the Services in this Contract, including technological, administrative or other types of improvements. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

2. Acknowledgements.

The parties acknowledge that:

(a) All Assets and Information Assets are subject to these Security Obligations.

(b) Notwithstanding any other provision of the Contract, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Assets and Information Assets.

3. Data Transfer and Retrieval.

The Contractor must, upon request by Canada:

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

(b) Securely transfer all Information Assets, including metadata, in a machine-readable and usable format acceptable to Canada, in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/Pages/guidelines-file-formats-transferring-information-resources-enduring-value.aspx).

4. Data Disposition and Returning Records to Canada.

(a) The Contractor must, upon request by Canada, securely dispose or reuse resources (e.g. equipment, data storage, files, and memory) that contain Information Assets and ensure that previously stored data cannot be addressed by others customers after it is released. This includes all copies of Information Assets that are made through replication for high availability and disaster recovery. The Contractor's disposal or reuse of resources must be aligned with one of the following: (i) National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); or (iii) Clearing and Declassifying

Electronic Data Storage Devices (CSE ITSG-06).

(b) The Contractor must, upon request by Canada, provide evidence that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from the Canada instance.

5. Continuous Monitoring.

(a) The Contractor must continually manage, monitor, and maintain the security posture of all Assets, Contractor Infrastructure and Service Locations throughout the period of the Contract, and ensure that the Public Cloud Services provided to Canada are in a manner that complies with these Security Obligations. As part of this obligation, the Contractor must:

(i) Actively and continuously monitor threats and vulnerabilities to its Assets, Contractor Infrastructure, Service Locations, or Information Assets;

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

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

(iv) Identify unauthorized use and access of any Public Cloud Services, data and components relevant to Canada's IaaS, PaaS or SaaS Solution;

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

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

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

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

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

6. Notifications.

(a) The Contractor must provide:

(i) Timely notification of any interruption that is expected to impact service availability and performance (as agreed to by the parties and included in the SOW and/or SLA);

(ii) Regular updates on the status of returning the Solution to an operating state according to the agreed upon SLAs and system availability requirements, both as advance alerts and post-implementation alerts; and

(iii) Information system security alerts, advisories, and directives via email for vulnerabilities that pose a threat to the Solution

7. Security Incident Response

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

(b) The Contractor must alert and promptly notify the Client (via phone and email) of any compromise, breach or of any evidence such as (i) a Security Incident, (ii) a security multifunction in any asset, (iii) irregular or unauthorized access to any Asset, (iv) large scale copying of an Information Asset, or (v) another irregular activity identified by the Contractor, that leads the Contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365 days), and will be made without undue delay, in any event, within 24 hours.

(c) The Contractor must collaborate with Canada on the containment, eradication, and recovery of Security Incidents in accordance with the Contractor's Security Incident response process and in alignment with the GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html). This includes:

(i) Allowing only designated representatives of Canada to have the ability to:

i. request and receive information associated with the Security Incident and any compromised Information Assets (including user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;

ii. track the status of a reported information security event or Security Incident.

(ii) Supporting Canada's investigative efforts in the case of any compromise of the users or data in the Solution that is identified.

(d) The Contractor must:

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

(ii) Track, or enable Canada to track, disclosures of Assets and Information Assets, including what data has been disclosed, to whom, and at what time.

8. E-Discovery and Legal Holds

The Contractor must (and must, to the extent applicable given the nature of the subcontracted Public Cloud Services provided by each Contractor Sub-processor, require Contractor Sub-processors to) take reasonable measures to ensure the Solution provides e-discovery and legal hold features for the Security Event Logs in order to enable Canada to conduct timely and effective security investigations and meet legal court requests for legal holds.

9. Security Assessment Testing

The Contractor must have a process that allows Canada to conduct a non-disruptive and non-destructive vulnerability scan or penetration test of Canada's portion of the Solution components within the Contractor environment.

10. Sub-processors

(a) The Contractor must provide a list of Sub-processors that could be used to perform any part of the Public Cloud Services in providing Canada with the Solution. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the Public Cloud Services that would be performed by the Sub-processor; and (iii) the location(s) where the Sub-processor would perform the Public Cloud Services.

(b) The Contractor must provide a list of Sub-processors within ten days of the effective date of the Contract. The Contractor must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14-days in advance of providing that Sub-processors with access to Client Data or Personal Information. The Contractor must assist Canada with verification of sub-processors within 10 working days.

11. Supply Chain Risk Management

Within 30 days of contract award, the Contractor must provide an up-to-date Supply Chain Risk Management (SCRM) Plan that has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime. The SRCM Plan must be provided to Canada on an annual basis, or upon request, or promptly following any material Change to the SRCM Plan.

APPENDIX C TO ANNEX C –

ADDITIONAL SECURITY INFORMATION FOR FOREIGN CONTRACTOR OR SUBCONTRACTOR

The Foreign Recipient **Contractor / Subcontractor** must perform a security screening of all its personnel who will need access to **CANADA PROTECTED i**nformation:

a) Identity check
    i. Copies of two of valid original pieces of government issued identity documentation, one of which must include a photo
    ii. Surname (last name)
    iii. Full given names (first name) – underline or circle usual name used
    iv. Family name at birth
    v. All other names used (aliases)
    vi. Name changes
        1. Must include the name they changed from and the name they changed to, the place of change and the institution changed through
    vii. Sex
    viii. Date of birth
    ix. Place of birth (city, province/state/region, and country)
    x. Citizenship(s)
    xi. Marital status/common-law partnership
        1. Current Status (married, common-law, separated, widowed, divorced, single)
        2. All current spouses (if applicable)
            a. Surname (last name)
            b. Full given names (first name) – underline or circle usual name used
            c. Date and duration of marriage/common-law partnership
            d. Date of birth
            e. Family name at birth
            f. Place of birth (city, province/state/region, and country)
            g. Citizenship

b) Residency check
    i. The last five (5) years of residency history starting from most recent with no gaps in time.
        1. Apartment number, street number, street name, city, province or state, postal code or zip code, country, from-to dates
c) Educational check
    i. The educational establishments attended and the corresponding dates.
d) Employment history check
    i. The last five (5) years of employment history starting from most recent with no gaps in time.
    ii. Three (3) employment reference checks from the last five (5) years.
e) Criminal records check:
    i. report(s) containing all criminal convictions for the last five (5) years in and outside of the candidate's country of residence.

ANNEX D

DEFINITIONS AND INTERPRETATIONS

In this Contract, unless the context otherwise requires, the following terms shall have the following meanings:

- **"ABAC"** or **"Attribute-Based Access Control"** means a logical access control methodology where authorization to perform a set of operations is determined by evaluating the attributes that are associated with the subject, object, requested operations, and in some cases, environment conditions against the policy, rules, or relationships that describe the allowable operations for a given set of attributes. (nist.gov)
- **"Active User"** means a registered user who has a user account and credentials to access the Solution.
- **"AD"** or **"Active Directory"** means a directory service developed by Microsoft for Windows domain networks to manage computers and other devices on a network. (microsoft.com)[1]
- **"Advanced Analytics"** means the autonomous or semiautonomous examination of data or content using sophisticated techniques and tools typically beyond those of traditional business intelligence (BI), to discover deeper insights, make predictions, or generate recommendations. Advanced analytics techniques include those such as data mining, text mining, machine learning, pattern matching, forecasting, visualization, semantic analysis, sentiment analysis, network and cluster analysis, multivariate statistics, graph analysis, simulation, complex-event processing, and neural networks. (Gartner.com)
- **"Advanced Search"** means a database search using methods such as proximity, wildcard, truncation, phrase matching, keyword matching or using Boolean operators to narrow ("and") or broaden ("or") to find stored information.
- **"AI"** or **"Artificial Intelligence"** means the application of advanced analysis and logic-based techniques including machine learning to interpret events, to support and automate decisions, and to take actions. (Gartner.com)
- **"AIA"** or **"Algorithmic Impact Assessment"** means a questionnaire designed to help designers assess and mitigate the risks associated with deploying an automated decision system. AIA provides designers with a measure to evaluate AI solutions from an ethical and human perspective, so that they are built in a responsible and transparent way. (Canada.ca)[2]
- **"API"** or **"Application Programming Interface"** means an interface that allows developers to interact with programs and applications including learning management systems.
- **"App"** means Application.
- **"Asset"** means all information technology resources used, accessed, or managed by the Contractor to provision and deliver the Services described in this Agreement (including—*without limitation*—all technology resources at the Contractor's Service Locations or at the Contractor's—*or a Contractor Subcontractor's*—data centre, networking, storage, servers, virtualization platforms, operating systems, middleware, and applications).
- **"ATP"** or "**Acceptance Test Plan**" means the acceptance testing process, such as the features to be tested, pass or fail criteria, approach to testing, checklists, roles and responsibilities, resource requirements and schedules. ATP also defines the functionality to be tested, the requirements verified by the test, test preconditions, test steps, and test post-conditions. Software testers determine if the software meets the customer's requirements, that is, it is ready for the customer to accept the software into their environment. (klariti.com)[3]

---

1 https://en.wikipedia.org/wiki/Active Directory

2 https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html

3 https://klariti.com/2018/09/24/what-is-an-acceptance-test-plan

- **"ATR"** or "**Acceptance Test Report**" means a report, primarily addressed to the software developers that summarizes the tests performed and their results. The ATR should attempt to classify the severity of each test non-conformity or failure and must identify each test uniquely. (ing.iac.es)[4]
- **"Authorized User"** means any user that holds a valid Solution access log-in profile with access defined by an RBAC or ABAC profile.
- **"Authorized User Access"** means the right granted to Canada by the Contractor to use the Solution and related services, as defined in the Statement of Work, in a Software as a Service (SaaS) or Hybrid distribution model. **"BCM"** or "**Business Capability Model**" means a document that represents high-level views of an organization from the perspective of its business capabilities and it briefly describes what an organization does. It is usually a high-level organization-wide set of business capabilities.
- **"BI"** or **"Business Intelligence"** means the applications, infrastructure and tools, and best practices that enable access to and analysis of information to improve and optimize decisions and performance (Gartner.com)
- **"Big Data Processing"** means techniques to analyze and systematically extract useful information from large scale data sets.
- **"BOLO"** or "**Be On the Lookout"** means a broadcast to law enforcement partners or within a law enforcement agency, that contains attributes identifying a suspect, person or other object of interest to law enforcement for the purposes of solving a crime or gaining criminal intelligence.
- **"Boolean Search"** uses connector words to combine search terms. There are three connectors: AND, OR, NOT
    - **AND**: Placed between words means both words should appear in each reference. This will narrow the search, by example renaissance AND music will retrieve all references which contain both terms.
    - **OR**: Placed between words means that either, or all, words may appear in each reference. This will broaden the search, by example earthquake OR seismology will retrieve all references with earthquake or seismology, as well as references with both terms.
    - **NOT**: Between words means that the second word should not appear in any reference. This will narrow the search, by example toxic NOT radioactive will retrieve all references with toxic, except references which include radioactive.
- **"Canada," "Crown," "Her Majesty,"** or **"the Government"** means Her Majesty the Queen in Right of Canada as represented by the Minister of Public Works and Government Services and any other person duly authorized to act on behalf of that Minister.
- **"Canada Data"** means information or data regardless of its form or format: (A) disclosed by or related to Canada's personnel, clients, partners, joint venture participants, licensors, vendors, or Contractors; (B) disclosed by or related to End Users of the Services; or (C) collected, used, or processed by, or stored for, the Services; which is directly or indirectly disclosed to the Contractor or Contractor Subcontractors by or on behalf of Canada or End Users.
- **"CAD"** means Canadian Dollar.
- **"CAFC"** or **"Canadian Anti-Fraud Centre"** means the central agency in Canada that collects information and criminal intelligence on such matters as mass-marketing fraud (by example, telemarketing), advance-fee fraud (by example, West African letter frauds), Internet fraud, and identification-theft complaints.
- **"CAR"** means Cybercrime Activity Report.
- **"Case Management"** means a complex process that requires a combination of human tasks and electronic workflow such as an incoming application, a submitted claim, a complaint, or a claim that is moving to litigation. This process may include workflow, management collaboration, storage of images and content, decisioning, and processing of electronic files or cases. (Gartner.com)
- **"CCCS" or "Canadian Centre for Cyber Security"** is a government organization that helps build Canada's cyber resilience and security through their advice, guidance, expertise, and partnerships. The

[4] http://www.ing.iac.es/~eng/standards/software/sof-std-4/node19.html

CCCS provides a single window for expert advice and services for governments, critical infrastructure operators, and the public and the private sector to strengthen their cyber security. (www.cyber.gc.ca)

- **"CCJS"** or "**Canadian Centre for Justice Statistics**" means the Centre within Statistics Canada which is the focal point of the federal-provincial-territorial collection of information on the nature and extent of crime and the administration of criminal justice in Canada. (publicsafety.gc.ca)[5]
- **"CEF"** or "**Common Event Format**" means an industry standard format, on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms.
- **"Certification"** means the action or process of providing someone or something with an official document attesting to a status or level of achievement. Some certifications are mandatory and condition to employment.
- **"CI/CD"** or "**Collaboration, Continuous Integration and Delivery**" means an agile methodology best practice because it enables software development teams to focus on meeting business requirements, code quality, and security because deployment steps are automated. CICD embodies a culture, a set of operating principles, and a collection of practices that enable application development teams to deliver code changes more frequently and reliably. (infoworld.com)[6]
- **"Client"** means the department or agency for which the Work or Services are performed under the Contract. In such respect, the Client may refer to any Government Department, Departmental Corporation or Agency, or other Crown entity described in the Financial Administration Act. (tpsgc-pwgsc.gc.ca)[7]
- **"Cloud Services"** means a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies. (Gartner.com)
- **"CSDM" or "Cloud Service Delivery Model"** means the manner in which the Cloud Service(s) are delivered to the consumer. Three fundamental models are defined; as Infrastructure (IaaS), as a Platform (PaaS) and as Software (SaaS). A CSDM can be comprised of any single one, or a combination of any or all models – known as a "Hybrid" CSDM.
- **"Complaint File"** means the Public Reporting Website that will capture cybercrime and fraud reports from the public or small and medium-sized businesses. Complaint Files are automatically ingested into the NCS Solution via an interface with the Public Reporting Website.
- **"Concept Search"** means searching based on a user specified concept(s) that describes documents to be returned as the search results. It can be a useful technique to identify potentially relevant documents when a set of keywords are not known in advance.
- •**"Concurrent Users"** means the total number of Authorized User simultaneously using (for example; querying, entering data, viewing, producing reports) the Solution at the same time. **"Containerization**" means the encapsulation or packaging up of software code and all of its dependencies so that it can run uniformly and consistently on any infrastructure. Containerization allows developers to create and deploy applications faster and more securely. Containerization allows applications to be written once and run anywhere. (ibm.com)
- **"Contract"** means the Articles of Contract, any general conditions, any supplemental general conditions, annexes, appendices, and any other document specified or referred to as forming part of the Contract, all as amended by agreement of the Parties from time to time.
- **"Contracting Authority"** means the person designated by that title in the Contract, or by notice to the Contractor, to act as Canada's representative to manage the Contract.
- **"Contractor"** means the entity named in the Contract to provide the Services or the Work to Canada.
- **"Correlation"** or **"Correlate"** means to identify a relationship between two or more pieces of information.

---

5 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/msrng-cnd/index-en.aspx

6 https://www.infoworld.com/article/3271126/what-is-cicd-continuous-integration-and-continuous-delivery-explained.html

7 https://www.tpsgc-pwgsc.gc.ca/comm/index-eng.html

- **"Cost"** means the cost determined according to Contract Cost Principles 1031-2 as revised to the date of the bid solicitation or, if there was no bid solicitation, the date of the Contract.
- **"COTS"** or **"Commercial Off-The-Shelf"** means software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf. (nist.gov)
- **"CPM"** means Contract Project Manager. This is the individual in the contractor organization responsible for the successful execution of the contract.
- **"CPU"** means Central Processing Unit that is the electronic circuitry within a computer that executes instructions that make up a computer program. The CPU performs basic arithmetic, logic, controlling, and input or output operations specified by the instructions in the program.
- **"CRM"** means Client Relationship Management.
- **"CRTC"** or "**Canadian Radio and Television Commission**" means an administrative tribunal that operates at arm's length from the federal government. The CRTC is dedicated to ensuring that Canadians have access to a world-class communication system that promotes innovation and enriches their lives. The CRTC's role is to implement the laws and regulations set by the Parliamentarians who create legislation and the departments that set policies. The CRTC regulates and supervises broadcasting and telecommunications in the public interest. (crtc.gc.ca)[8]
- **"CSE"** means Communications Security Establishment. This is the Government of Canada's national cryptologic agency. Administered under the Department of National Defence, it is responsible for foreign signals intelligence and protecting Canadian government electronic information and communication networks.
- **"CSP"** or **"Cloud Service Provider"** means the entity that owns, operates, and maintains the physical infrastructure ("Cloud") and provides virtualized computing resources to consumers. The CSP can provide basic information technology infrastructure such as compute and data storage or complete solutions as hosted software.
- **"CUA"** means Capability and Usability Assessment. CUA is used to analyse the capability of a development organisation in performing user-centred design.
- "**Cyber**" means the Internet and information technologies such as computers, tablets, or mobile devices.
- **"Cybercrime"** means any crime where cyber—the Internet and information technologies such as computers, tablets, or mobile devices—is instrumental to committing a criminal offence. The RCMP breaks cybercrime into two categories: Technology-as-target where the crime can only be committed using computers, networks, and digital devices, and Technology-as-instrument where the Internet and information technologies play an instrumental role in the crime. (rcmp-grc.gc.ca)
- **"Cybercrime Taxonomy"** means the taxonomy that provides a consistent language across North American law enforcement agencies in an effort to increase reporting, documentation, and intelligence sharing as well as to further legislation and enable comparable statistical analysis.
- **"Cybersecurity"** means a combination of people, policies, processes, and technologies that are employed by an enterprise to protect its cyber assets. (Gartner.com)
- **"Data Custodian"** means a person or organization that is in possession or control of computer data. Relevant to processing a preservation request, demand, or order.
- **"Data Preservation Demand"** means a demand made by a Peace Officer or Public Officer under Criminal Code of Canada s.487.012, that requires the preservation of specified computer data by the person in possession or control of that data. Data Preservation Demands issued on behalf of a foreign jurisdiction expire 90 days after they are issued to the Data Custodian. Data Preservation Demands issued by a Canadian Law Enforcement agency expire 21 days after they are issued to the Data Custodian. Data Preservation Demands can be issued once for the information meaning that a Preservation Demand cannot be renewed.
- **"Data Preservation Order**" means a court-issued order made by a Peace Officer or Public Officer under Criminal Code of Canada s.487.013 that requires that computer data that is in possession or control of a

---

8 https://crtc.gc.ca/eng/home-accueil.htm

person be preserved by that person. Prior to issuance, a Data Preservation Order must first be sworn before a Justice of the Peace or Judge. Data Preservation Orders expire 90 days after they are issued to the Data Custodian. Data Preservation Orders can be renewed.

- **"Data Preservation Request"** means a request to preserve data that is made to Canada from a foreign jurisdiction or is made from Canada to a foreign jurisdiction. Data Preservation Demands and subsequent Data Preservation Orders are created and managed by the NC3 24/7 Point of Contact based on Data Preservation Requests and requests for extension received from foreign jurisdictions.
- **"DBMS"** means Database Management System.
- **"Deconflict"** means to adjust or coordinate to prevent or resolve conflict (by example, if several Police Agencies are interested in a Network Server, deconfliction implies the identifying and mitigating of their mutual interests).
- **"Deliverable"** or **"Deliverables"** means in a generic sense, any discrete part of the Work to be performed for Canada.
- **"Device"** means equipment having a physical central processor unit (CPU), mass storage, input and output devices (by example, keyboard, mouse, microphone, and monitor), and includes servers, desktops, workstations, notebooks, laptops, personal digital assistants, and mobile computing equipment.
- **"DevOps"** is a set of practices that combines software development (Dev) and information-technology operations (Ops) which aims to shorten the systems development life cycle and provide continuous delivery with high software quality.
- **"DHCP"** means Dynamic Host Configuration Protocol that is a network management protocol used on Internet Protocol networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.
- **"Diary Date"** means a system date and time stamp applied to notes and memos.
- **"Disclosure Package"** means the ability to identify, assess and select the material from a File or Project including records, forms, statements, reports, data and activities, to prepare a document package for presentation to Police Partners or in court.
- **"DRP"** means Disaster Recovery Plan.
- **"DNS"** means Domain Name System means a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
- **"Drill down"** means to access data which is in a lower level of a hierarchically structured database.
- **"DSB"** means the RCMP Departmental Security Branch.
- **"Dublin Core Standard for Metadata"** is a small set of pre-defined vocabulary terms that can be used to describe web resources (video, images, web pages, etc.), as well as physical resources such as books or CDs, and objects like artworks. They offer expanded cataloging information and improved document indexing for search engine programs.
- **"DSCP"** means the RCMP Departmental Security Control Profile.
- **"EC3"** or **"European Cybercrime Coordination Centre"** means the Europol body that co-ordinates cross-border law enforcement activities against computer crime and acts as a centre of technical expertise on the matter. The EC3 was set up in 2013 to bolster the response of law enforcement to cybercrime in the EU and help protect European citizens, businesses, and governments. Each year, the EC3 issues the Internet Organised Crime Threat Assessment, its flagship strategic report on key findings and emerging threats and developments in cybercrime. (europol.europa.eu)[9]
- **"End User"** means any Authorized User with access to the National Cybercrime Solution.
- **"Enrichment"** means to add value by correlation, aggregation, enquiry, analysis, and collation of results.

[9] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

- **"Entity"** means any object in a database that we want to model and store information about. Entities are usually recognizable concepts, either concrete or abstract, such as person, places, things, or events which have relevance to the database. Some specific examples of entities are Persons, Vehicles, Locations, Organizations, Phone Numbers, Exhibits, etc., which have data associated to them.
- **"Error"** means any instruction or statement that is contained in—*or is absent from*—the Solution that by its presence—*or its absence*—prevents the Solution from operating in accordance with the Specifications.
- **"ETL"** means Extract, Transform, Load which is the general procedure of copying data from one or more sources into a destination system which represents the data differently from the source(s) or in a different context than the source(s).
- **"ESRI"** means Environmental Systems Research Institute that is a provider of enterprise geographic information system solutions.
- **"Europol"** means the European Union's law enforcement agency means the law enforcement agency of the European Union (EU) formed in 1998 to handle criminal intelligence and combat serious international organised crime and terrorism through cooperation between competent authorities of EU member states. (europol.europa.eu)[10]
- **"Europol Handling Codes"** means the Handling Codes defined by Europol to convey the wishes of the provider of the information with respect to sharing and security of the information. Handling codes include:
  - H1 - Information must not be used as evidence in judicial proceedings without permission of the provider;
  - H2 - Information must not be disseminated without the permission of the provider; and
  - H3 - Other restrictions apply and should be included as text instructions.
- **"Exact Phrase Search"** means when a string of words are searched for as an exact phrase. References will be retrieved only if the words occur side by side, (by example, information technology). In some databases, phrase searching requires the phrase to be enclosed in quotation marks, (by example, "information technology").
- **"Exploitive Material"** means material that is likely to cause offence to a reasonable adult, describes or depicts a person or a representation of a person who is or apparently is a child under the age of 16 years.
  - in a sexual context, including for example, engaging in a sexual activity; or
  - in an offensive or demeaning context; or
  - being subjected to abuse, cruelty or torture.
- **"External User"** means an Authorized Police and Partner Portal (P3) User.
- **"FBI"** means Federal Bureau of Investigation is the domestic intelligence and security service of the United States and its principal federal law enforcement agency.
- **"FBI IC3"** means FBI Internet Crime Complaint Centre whose mission is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.[11]
- **"File"** means a concept of a Ticket that has been assessed and deemed appropriate (meets mandate, severity and priority requirements) for processing by the NC3. Files may contain many Tickets or may be related to each other.
- **"FINTRAC"** or **"Financial Transaction and Report Analysis Centre of Canada"** means Canada's financial intelligence unit. Its mandate is to facilitate the detection, prevention, and deterrence of money laundering and the financing of terrorist activities while ensuring that the protection of personal information under its control.

---

10 https://www.europol.europa.eu/about-europol

11 https://www.ic3.gov/about/default.aspx

- **"FOC"** or **"Full Operating Capability"** means the capabilities described in the BCM are fully delivered and being utilized by the NC3 Unit and other stakeholders to conduct business operations.
- **"Full Text Search"** means techniques for searching a single document or a collection in a full text or document database based on user specified criteria. In a full-text search, the search engine examines all the words in every stored document as it tries to match search criteria.
- **"Fuzzy Search"** means a process that locates information that is likely to be relevant to a search criterion even when it does not exactly correspond to the search result. Exact and highly relevant matches appear near the top of the list. Subjective relevance ratings, usually as percentages, may be given.
- **"GB"** means Gigabyte that is a unit of computer information consisting of 1,024 megabytes.
- **"GC"** or "GOC" means Government of Canada.
- **"GC Digital Standards"** or **"Government of Canada Digital Standards"** are the foundation of the Government of Canadian's shift to becoming more agile, open, and user-focused. They guide teams in designing digital services in a way that best serves Canadians. (Canada.ca)
- **"GUI"** means Graphical User Interface that is a form of user interface that allows users to interact with electronic devices through graphical icons and audio indicator such as primary notation, instead of text-based user interfaces, typed command labels or text navigation.
- **"GIS"** means Geographic Information System.
- **"HOST"** is the premier symposium that facilitates the rapid growth of hardware-based security research and development. Since 2008, HOST has served as the globally recognized event for researchers and practitioners to advance knowledge and technologies related to hardware security and assurance.
- **"HQ"** means Headquarters.
- **"HTML"** means Hypertext Markup Language that is the standard markup language for documents designed to be displayed in a web browser.
- **"IaaS"** or **"Infrastructure as a Service"** means a cloud service delivery method whereby a Cloud Service Provider provides the consumer with fundamental computing resources such as servers, processing, storage, and networking upon which the consumer can deploy and run arbitrary software which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly has limited control of select networking components (by example, host firewalls).
- **"IaaS Infrastructure"** means Infrastructure managed by the Consumer and provided as a Service (by example, Data Center, Networking, Storage, Servers, Virtualization platform) and includes the systems, hardware, and software that are used to manage, operate, and provision an IaaS Infrastructure.
- **"IBM"** means International Business Machines Corporation.
- **"IDS" or "IPS"** means Intrusion Detection System or Intrusion Prevention System. It is a device or a software application that monitors a network or systems for malicious activity or policy violations.
- **"ILM"** means Information Lifecycle Management.
- **"IM" or "IT"** means Information Management or Information Technology.
- **"Information Assets"** means any individual data element of such Canada Data.
- **"Information Spillage"** means incidents where an Information Asset is inadvertently placed on an Asset or System that is not authorized to process it (by example, ITSG-33, IR-9).
- **"Initial Operating Capability"** means an interim operating solution that is implemented to allow the NC3 Unit to conduct their operations until such a time that the Solution being developed is in place.
- **"INTELEX"** means a national information query program operated by the RCMP. INTELEX queries are distributed to various regional or divisional INTELEX units where local systems are queried. Results are collected and returned to the requester.
- **"Internal User" or "Core User"** means an NCS user who is accessing the Solution directly – not via the Police and Partner Portal. Internal Users will primarily consist of RCMP resources such as NC3 Unit employees and IM/IT, National Division or Tech Ops resources.

- **"Interoperability"** means the extent to which hardware and software elements work together.
- **"IOC"** or **"Indicators of Compromise"** means forensic evidence that indicates (with high confidence) a computer intrusion. Typical IOCs are virus signatures, IP addresses, MD5 hashes of malware files, or URLs or domain names of botnet command and control servers.
- **"IP"** means Internet Protocol that is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.
- **"ISO"** means International Organization for Standardization.
- **"ISP"** means Internet Service Provider that is an organization that provides services for accessing or using the Internet. Internet service providers can be organized in various forms, such as commercial, community-owned, non-profit, or privately owned.
- **"IT"** means Information Technology
- **"ITCP"** means Information Technology Continuity Plan.
- **"IT Security"** or **"Information Technology Security"** means a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. (Cisco.com)
- **"ITSG"** means Information Technology Security Guidance.
- **"ITSP"** means Information Technology Security Guidance for the Practitioner.
- **"J-CAT"** or **"Joint Cybercrime Action Task Force"** is made up of a standing team of cybercrime liaison officers from European Union (EU) Member States and non-EU partner countries. There are 13 law enforcement agencies from 11 countries who have access to Europol's cybercrime intelligence databases. J-CAT works on cybercrimes with a nexus to Canada including malware, botnets and intrusion, online money laundering, crypto currencies, and cyber fraud. Hosted by the European Cybercrime Coordination Centre (EC3), its mission is to drive intelligence-led, co-ordinated action against key cybercrime threats through cross-border investigations and operations by its partners.
- **"JPEG"** or **"Joint Photographic Experts Group"** is a commonly used method of lossy compression for digital images, particularly for those images produced by digital photography. The degree of compression can be adjusted, allowing a selectable trade-off between storage size and image quality.
- **"JSON"** means JavaScript Object Notation that is a language-independent data format that uses human-readable text to store and transmit data objects consisting of attribute or value pairs and array data types.[12]
- **"KB"** means kilobyte that is a multiple unit used for binary data. Although "kilo" generally refers to 1,000, in computer science, one kilobyte often refers to 1,024 bytes. This measure is often used to describe memory capacity and disk storage.
- **"Keyword Search"** means searching using keyword terms used to identify the content of documents. Using the keyword terms can make searching easier and more reliable.
- **"LE"** means Law Enforcement that means any system by which some members of government act in an organized manner to enforce the law by discovering, deterring, rehabilitating, or punishing people who violate the rules and norms governing that society.
- **"LEIDS"** means Law Enforcement Information Data Standards. The Canadian Association of Chief of Police (CACP) has created LEIDS as an operational committee to drive data exchange interoperability based upon NIEM.
- **"Maintenance Releases"** means all commercially available enhancements, extensions, improvements, upgrades, updates, releases, versions, renames, rewrites, cross-grades, components and back grades or other modifications to the Solution developed or published by the Contractor or its licensor.

---

12 https://en.wikipedia.org/wiki/JSON

- **"Malware"** means software that is intentionally included or inserted into a system for a malicious purpose and done so without the owner's approval. Common forms of malware include viruses, worms, Trojans, spyware, scareware, diallers, rootkits, exploit kits, and ransomware.
- **"Malware Sample"** means malicious code that has not been altered through the efforts of automated virus and malware scanners thereby providing law enforcement and malware analysis service organizations with pristine samples for analysis and hashing.
- **"Malware Analysis Service"** means a service provided by an external organization that as a minimum, maintains a library of malware hash values. In addition, the service could perform an analysis of a malware sample and provide a report detailing the results of this analysis. Examples of malware analysis service organizations include CCCS, FBI, and EMAS.
- **"Manage"** means in the context of an information system, actions such as the creation of, modification of, deletion of, and access to information or records.
- **"Message"** means a communication from the system or user that contains information, actions, or responses.
- **"MC"** means Mandatory Criteria.
- **"Metadata"** means data that provides information about other data.
- **"MFA"** means Multi-Factor Authentication that is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism.
- **"MISP"** or **"Malware Information Sharing Platform"** means a free, open-source software, threat-sharing platform that facilitates the information sharing of threat intelligence including cyber security indicators. MISP is a threat-intelligence platform for gathering, sharing, storing, and correlating the Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information, or even counter-terrorism information.
- **"ML" or "Machine Learning"** means a subset of Artificial Intelligence that uses statistical models that can extract knowledge and patterns from data in order to solve problems.
- **"MLAT"** or **"Mutual Legal Assistance Treaty"** is an international agreement between States (Governments) in written form, governed by international law. MLATs provide a vehicle through which countries, such as Canada, receive and provide assistance in the gathering of evidence for use in criminal investigations and prosecutions. MLAT is an agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws. Modern states have developed mechanisms for requesting and obtaining evidence for criminal investigations and prosecutions.
- **"MVP"** or **"Minimal Viable Product"** means a Prototype Solution that minimally delivers the requirements for the five (5) CUA Scenarios in Appendix A to Annex A.
- **"NC3"** or **"National Cybercrime Coordination Unit"** mean a unit composed of both RCMP officers and civilians from a variety of backgrounds. The NC3 will work with law enforcement and other partners to help reduce the threat, impact and victimization of cybercrime in Canada. (rcmp-grc.gc.ca)
- **"NCECC"** or **"National Child Exploitation Coordination Centre"** functions as the point of contact for investigations related to the sexual exploitation of children on the Internet in Canada. The NCECC is Canada's main portal for all matters related to the sexual exploitation of children on the Internet, including those destined for international agencies and those originating from foreign agencies and destined for Canada. The NCECC validates international requests, prepares, and disseminates investigative packages to the proper jurisdiction within Canada.
- **"NCFRS"** or **"National Cybercrime and Fraud Public Reporting Website and System"** refers to the Public Reporting Website being developed as part of the overall NCS. NCFRS will be used by the Canadian public and small to medium-sized businesses to report cybercrimes and frauds.
- **"NCFTA"** or **"National Cyber-Forensics & Training Alliance"** is a non-profit corporation founded in 2002, focused on identifying, mitigating and neutralizing cybercrime threats globally. The NCFTA operates by conducting real time information sharing and analysis with Subject Matter Experts (SME) in the public,

private and academic sectors. Through these partnerships, the NCFTA proactively identifies cyber threats in order to help partners take preventive measures to mitigate those threats.

- **"NCS"** means National Cybercrime Solution.
- **"NCS-PE"** means NCS Production Environment.
- **"NCS-TE"** means NCS Test Environment.
- **"NIEM"** or **"National Information Exchange Model"** is a common vocabulary that enables information exchange across diverse public and private organizations. NIEM connects communities of people who share a common need to exchange information in order to advance their mission. NIEM is viewed as a dictionary of agreed-upon terms, definitions, relationships, and formats that are independent of how information is stored in individual systems.
- **"NLP"** or **"Natural-language Processing"** means technology that involves the ability to turn text or audio speech into encoded, structured information, based on an appropriate ontology.
- **"Notification"** means an email to a user or a group that a message or task has been sent or made available to them.
- **"OAuth"** provides to clients a "secure delegated access" to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials.
- **"Observable"** See Indicators of Compromise.
- **"OCR"** or **"Optical Character Recognition"** means a process or component that extracts text from images of printed or handwritten letters.
- **"OGD"** or **"Other Government Departments"** means other federal government departments and agencies other than the RCMP**.**
- **"Official Languages Act"** is a Canadian law that came into force on September 9, 1969, which gives French and English equal status in the government of Canada.
- **"Open-source"** means software that comes with permission to use, copy, and distribute, either as is or with modifications and that may be offered either free or with a charge. The source code must be made available. (Gartner.com)
- **"OpenID"** means Open standard and decentralized authentication protocol. it allows users to be authenticated by co-operating sites using a third-party service, eliminating the need for webmasters to provide their own ad hoc login systems, and allowing users to log into multiple unrelated websites without having to have a separate identity and password for each.
- **"OS"** means Operating System that is a system software that manages computer hardware, software resources, and provides common services for computer programs.
- **"OSINT"** or **"Open Source Intelligence"** is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or public intelligence.
- **"P3"** or **"Police and Partner Portal"** means the externally facing portal that provides a secure means of communication between NC3 and Canadian Police and authorized Cybercrime Partners. Access to the P3 is strictly controlled via RBAC. The P3 is enables external queries to the NCS Data Repository as well as submission of cybercrime data, cases and service requests. The P3 is also used by the NC3 to make cybercrime Public reports available to PoJ and exchange information with Police and Partners.
- **"P3 User"** means a user authorized to use the Police and Partner Portal component of the NCS.
- **"PaaS"** or **"Platform as a Service"** is a Cloud Service delivery method whereby a Cloud Service Provider (CSP) provides a platform on which the consumer can build, deliver and support applications and services over the Internet. Servers, Operating System and other services such as Database, Middleware is managed by the CSP.
- **"Private PaaS"** means a PaaS is downloaded and hosted on the RCMP Cloud Tenant.

- **"Public PaaS"** means a PaaS is hosted by a Cloud Service Provider (CSP)
- **"PB"** means Protected B.
- **"PDF"** means Portable Document Format that is a file format that has captured all the elements of a printed document as an electronic image that you can view, navigate, print, or forward to someone else.
- **"Personal Information"** means information that is about an identifiable individual and recorded in any form, as defined in section 3 of the Privacy Act. Examples include, but is not limited to the information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial, or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual. Definition from Government of Canada Justice Laws Website: https://laws-lois.justice.gc.ca/eng/acts/P-21/section-3.html
- **"PIA"** means Privacy Impact Assessment that is a type of impact assessment conducted by an organization; typically, a government agency or corporation with access to a large amount of sensitive, private data about individuals in or flowing through its system. It assists organizations in identifying and managing the privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships.
- **"Pick List"** mean a list of choices (displayed as a list) that can be displayed within a user interface and from which normally only one item may be selected.
- **"PKI"** means Public Key Infrastructure. Its aim is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method.
- **"PNG"** or **"Portable Network Graphics"** is a raster-graphics file format that supports lossless data compression. PNG was developed as an improved, non-patented replacement for Graphics Interchange Format (GIF).
- **"PO"** or "Project Office" sometimes referred as project management office. Its role is to offer support and information on the planning, monitoring and reporting on the health of the project to facilitate decision making in a timely fashion.
- **"POJ"** or **"Police of Jurisdiction"** means a police agency with the jurisdiction in which a crime was possibly committed or is under investigation.
- **"PoP"** or **"Prototype on Platform"** is a test of the contractor's solution to confirm that it will function as described per the contractor's solution cloud service delivery model
- **"Power User"** means a user whose skills and expertise are more advanced than most other users, especially a person with administrative rights and responsibilities related to the Solution and NC3.
- **"PRC"** refers to rated requirements for corporate qualifications and project management.
- **"PRF"** refers to rated requirements for functional capabilities.
- **"PRM"** means Progress Review Meetings whose purpose is to obtain an update on the status of project activities and identify problems areas of a project that require management actions, decisions or escalation.
- **"Production Order"** means a judicial authorization that compels a person, including an organization, to disclose documents and records to an authorized peace officer.
- **"Project"** means a concept of a larger undertaking or File that involves more personnel, partners, time, resources, outcomes and reports. A Project may contain links to several Files. A Project could be used to manage activities and resources related a specific cybercrime campaign or major event that requires coordination amongst several agencies.
- **"Project Close Out"** means the process involving the following activities: the Client verifies that the final product or work is satisfactory; the Client ensures that the contractor has been paid; the Client begins administrative closure of the contract which includes verifying the cost, making a final amendment to the contract; and closing the project. For more information, refer to the PWGSC Supply Manual, Chapter 8:

Section 8.175 Contract End and Contract Close Out[13] and Annex 8.1: Guidelines on File Organization and Make-up.[14] (buyansell.gc.ca)[15]

- **"PROS"** or **"Police Reporting and Occurrence System"** means the Record Management System (RMS) that is used by the RCMP.
- **"Proximity Search"** means searching for two or more words that occur within a certain number of words from each other.
- **"PRT"** refers to rated requirements for technical capabilities.
- **"PRV"** refers to rated requirements for video demonstration.
- **"PSPC"** or **"Public Services and Procurement Canada"** or **"Public Works and Government Services Canada"** means the Public Services and Procurement Canada as established under the Department of Public Works and Government Services Act.
- **"QA"** or **"Quality Assurance"** is a way of preventing mistakes and defects in manufactured products and avoiding problems when delivering products or services to customers; which ISO 9000 defines as "part of quality management focused on providing confidence that quality requirements will be fulfilled".[16]
- **"QC"** or "**Quality Control**" means ensuring that hardware, software and deliverables meet the standards established by the enterprise at the point of delivery.
- **"RBAC"** or **"Role-Based Access Control"** means access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. (nist.gov)
- **"RCMP"** means Royal Canadian Mounted Police that is Canada national police service, providing law enforcement at the federal level. The RCMP also provides provincial policing in eight of Canada's provinces (Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Prince Edward Island, and Saskatchewan, i.e., all except Ontario and Quebec) and local policing on a contract basis in the three territories (Northwest Territories, Nunavut, and Yukon) and more than 150 municipalities, 600 aboriginal communities, and three international airports.
- **"RCMP Cloud Tenant"** means the Protected B Public Cloud IaaS public cloud resources purchased from a CSP and managed by the RCMP.
- **"RDBMS"** means Relational Database Management System. It refers to a database that stores data in a structured format, using rows and columns. This makes it easy to locate and access specific values within the database. It is "relational" because the values within each table are related to each other. The relational structure makes it possible to run queries across multiple tables at once.
- **"Record"** means any hard copy document or any data in a machine-readable format containing Personal Information or Canada data.
- **"Redaction"** means to hide ore remove parts of a text before publication or distribution.
- **"Red Hat"** is an open-source software company.
- **"Regex"** means a regular expression that is a sequence of characters that define a search pattern. Usually such patterns are used by string searching algorithms for "find" or "find and replace" operations on strings, or for input validation. It is a technique developed in theoretical computer science and formal language theory. (Wikipedia.org)

---

13 https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/8#section-8.175

14 https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/8#annex-8.1

15 https://buyandsell.gc.ca/for-government/buying-for-the-government-of-canada/manage-the-contract/contract-close-out

16 https://en.wikipedia.org/wiki/Quality_assurance

- **"REST"** means Representational State Transfer that represents an architectural style for providing standards between computer systems on the web, making it easier for systems to communicate with each other.
- **"RFP"** means Request for Proposal that is a document that solicits proposal, made through a bidding process, by an agency interested in procuring a commodity, service, or valuable asset, to potential suppliers to submit business proposals.
- **"RMS"** or **"Records Management System"** means an IT system used by law enforcement to manage occurrences, case data, investigations, criminal booking and other related data.
- **"RPO"** or **"Recovery Point Objective"** refers to the maximum targeted time an application can be down without causing significant damage to the business.
- **"RTO"** or **"Recovery Time Objective"** refers to how much time an application can be down without causing significant damage to the business.
- **"SAML"** means Security Assertion Markup Language that is an open standard that allows identity providers to pass authorization credentials to service providers. In other words, a user can use one set of credentials to log into many different websites.
- **"Sandbox"** means the NC3 Cybercrime Analysis Sandbox that can be used by NC3 internal users and via the Police and Partner Portal to perform analysis on a variety of cybercrime related files.
- **"SA&A"** means Security Assessment and Authorization which is the mechanism by which risk to an IT system is understood, mitigated, and consistently and measurably managed throughout its lifecycle.
- **"SaaS" or "Software as a Service"** is a software distribution model in which the customer pays via subscription for access to an application that is hosted by a Cloud Service Provider (CSP). The service is made available over the Internet.
- **"SCED"** means Secure Cloud Enablement and Defence. Its objective is to implement Government of Canada (GC) Trusted Interconnection Points on the periphery of the GC network for the secured exchange of data with external organizations.[17]
- **"SDD"** means System Design Document that is a deliverable associated with the vendor proposed solution.
- **"Security Event Log"** means any event, notification or alert that a device, systems or software is technically capable of producing in relation to its status, functions and activities. Security Events Logs are not limited to security devices, but are applicable to all devices, systems and software that are technically capable of producing event logs that can be used in security investigations, auditing and monitoring.
- **"Security Incident"** means any observable or measurable anomaly occurring with respect to an Asset, which results, or which may result, in: (A) a violation of the Canada's Security Policies, a Specific Security Measure, the Contractor's or Subcontractor's security policies or procedures, or any requirement of these Security Obligations or the Privacy Obligations; or (B) the unauthorized access to, modification of, or exfiltration of any Authorized Personnel's credentials, Users' credentials, or Information Asset.
- **"Service Request"** means a request to the NC3 Unit from a partner agency. Some Requests for Service can be submitted as structured transactions via the Police and Partner Portal. Many Requests for Service may be ad hoc in nature, received by email, telephone, internally generated, or Police and Partner Portal. Examples of Requests for Service include requests to:
    - Submit data to the NCS Data Repository;
    - Query the NCS Data Repository;
    - Flag data for monitoring (i.e., BOLO);
    - Share a bulletin or notify the NC3 Unit of an incident;
    - Request Preservation of Data in a foreign jurisdiction;

[17] https://www.canada.ca/en/shared-services/corporate/publications/2019-20-departmental-plan/supplementary-tables/status-report-secure-cloud-enablement-defence.html

- Provide guidance or access to expertise;
- Request for Intelligence analysis;
- Request for assistance on specific cybercrime and fraud investigations; and
- Requests for access to forensic software tools to fight cybercrime and fraud.

- "**Services**" means:
  - Granting Solution access and usage rights;
  - Providing Solution Documentation;
  - Maintaining, upgrading, and updating the Solution;
  - Managing incidents and defects to ensure the Solution(s) operate at the applicable service levels; and
  - Providing incidental and additionally required information technology infrastructure services required to deliver the Solution.
- **"SIEM"** means Security Information and Event Management a subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.
- **"SIENA"** means Secure Information Exchange Network Application. SIENA is a state-of-the-art platform that meets the communication needs of EU law enforcement. [18]
- **"Silent Hit"** means that the data contributor will receive an automatic electronic notification of a query while the querying agency does not receive a matching record in the query result if the query result contains data that is tagged for Silent Hit treatment.
- **"Silent Query"** means a query resulting in one or more notifications of correlations are to be returned to the querying agency only and not to other agencies such as the data contributor or agencies having a Watch List entry for the subject of the query.
- **"Single Sign-On"** means a set of credentials that allows users to access multiple applications in your organization while only needing the user to sign in once.
- **"SKU"** or **"Stock Keeping Unit"** is a product code that can be used to search and identify stock on hand from lists, invoices, or order forms. It is typically used in inventory management.
- **"SMB"** or **"Small to Medium-Sized Businesses"** means a business that due to its size has different IT requirements and which often faces different IT challenges than do large enterprises, and its IT resources (i.e., usually budget and staff) are often highly constrained. (Gartner.com)
- **"SME"** means subject matter expert.
- **"SMS"** means Short Message Service.
- **"SOAP"** means Simple Object Access Protocol that is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to provide extensibility, neutrality, verbosity and independence.
- **"Solution Availability"** means the percentage of minutes in a month that the Solution is operational.
- **"Solution Technical Documentation"** means all of the manuals, handbooks, user guides, and other human-readable material to be provided by the Contractor to Canada under the Contract for use with the Solution.
- **"SOS"** means Statement of Sensitivity.
- **"SOW"** means Statement of Work document. It is the narrative description of a project's work requirement. It defines project-specific activities, deliverables and timelines for a vendor providing services to the client.

---

[18] https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena

- **"Speech-to-Text"** that is a type of software that effectively takes audio content and transcribes it into written words in a word processor or other display destination. This type of speech recognition software is extremely valuable to anyone who needs to generate a lot of written content without a lot of manual typing.
- **"Specifications"** means the description of the essential, functional, or technical requirements of the Services in a Statement of Work, including the procedures for determining whether the requirements have been met.
- **"SPROS"** or **"Secured Police Reporting and Occurrence System"** is a version of PROS with enhanced security features and restricted access. SPROS is used for National Security and Critical Infrastructure incidents.
- **"SQL"** means Structured Query Language that is a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system.
- **"SRTM"** means Security Requirements Traceability Matrix. This is a document that links system security requirements throughout the validation process. The SRTM ensures that all security requirements defined for a system are tested and not lost during the final acceptance of the Solution.
- **"SSC"** means Shared Services Canada is an agency of the Government of Canada responsible for providing and consolidating information technology services across federal government departments.
- **"SSO"** or **"Single Sign-On"** means a set of credentials that allows users to access multiple applications in your organization while only needing the user to sign in once.
- **"STIX"** or **"Structured Threat Information eXpression"** is a structured language and serialization format used to exchange cyber threat intelligence. It enables organizations to share cyber threat intelligence with one another in a consistent and machine-readable manner. STIX allows security communities to better understand what computer-based attacks they are most likely to see and to anticipate or respond to those attacks more effectively. STIX is designed to improve many different capabilities such as collaborative threat analysis, automated threat exchange, automated detection and response, etc.
- **"STT" or "Speech-to-Text"** that is a type of software that effectively takes audio content and transcribes it into written words in a word processor or other display destination. This type of speech recognition software is extremely valuable to anyone who needs to generate a lot of written content without a lot of manual typing.
- **"Submissions"** refers to Data Submissions, Intelligence Submissions, and Complaint File Submissions and described below:
    - **"Data Submission"** means a submission that contains raw information or data with general context but may or may not contain actionable information. The submission may or may not contain discoverable Intelligence;
    - **"Intelligence (or "intel") Submission"** means a submission that contains potentially actionable information that can be used operationally or be referred to a Law Enforcement agency. Intelligence submissions will undergo assessment to confirm releasability and reliability by an Intelligence Analyst; and
    - **"Complaint File Submission"** means a submission that is generated by the Public Reporting Website based on a report from the public or from small and medium-sized businesses. It should be noted that public cybercrime and fraud reports could also originate from call-in "interview" scenarios between victim or complainant and a Call Centre operator.
- **"Support"** refers to the four (4) levels of support that the Solution requires:
    - **Level 0** – Ask super-user
        - Automated or self-service solutions (e.g. Chatbots) that users can access themselves without the aid of the RCMP Central Help Desk. These include automated password resets, knowledge base including detailed product and technical information and application manuals. Level 0 support is performed without the aid of the RCMP Central Help desk technician.
    - **Level 1** – RCMP

        - Central Help desk filters calls and provides basic support and troubleshooting, such as password resets, how-to instructions, Service Desk Management (SDM) ticket routing and escalation to Level 2 and Level 3 support. A Level 1 Support Technician gathers and analyses information about the user's issue and determines the best way to resolve their problem. Level 1 may also provide support for identified Level 2 and Level 3 issues where configuration solutions are documented. Frequently asked questions (FAQ) and Operation procedures are used to reduce escalation and provide user training.
    - **Level 2** – RCMP
        - Handles In-depth technical support relating to configuration issues, troubleshooting, software installations, hardware repair, database administration and Route Cause Analysis. Handles escalated issues that Level 1 Support Technician is not equipped to handle. Level 2 can escalate to Level 3 after all documented avenues to solving the problem have been reviewed. Can research and implement fixes for new issues and only escalate to Level 3, if it is out of their skill set or ability to solve.
    - **Level 3** – RCMP/Contractor
        - Subject matter experts (SME) attempt to duplicate the problems and define root causes, using product designs, code, or specifications, create necessary enhancements, hot fixes & patches, and deliver release packages. A Level 3 Support Technician has the most IT expertise and is the SME for solving undocumented issues.
- **"SUS"** or **"System Usability Scale"** is a simple, ten-item attitude Likert scale giving a global view of subjective assessments of usability.
- **"SuSE"** or **"Software und System-Entwicklung"** is a commercial Linux operating system.
- **"Task"** means a piece of work to be done or undertaken. Tasks are created and assigned as a request to an individual or a team. The individual is then responsible for completing the Task. Supervisors manage the progress of a task until completion or pended or referred if necessary.
- **"TAXII"** or **"Trusted Advance eXchange of Indicators Information"** means a definition for how cyber threat information can be shared via services and message exchanges.
- **"TB"** or **"Terabyte"** is a multiple of the unit byte for digital information. The prefix tera represents the fourth power of 1000 and therefore one terabyte is one trillion (short scale) bytes.
- **"TBS"** means Treasury Board of Canada Secretariat. It provides advice and makes recommendations to the Treasury Board committee of ministers on how the government spends money on programs and services, how it regulates and how it is managed.
- **"Technical Support User"** means a User who can provide support services to resolve System related issues or to Users in need of technical or Solution usage related assistance.
- **"Ticket"** means a concept of a Service Request or Submission that has been received where a decision to take action has not yet been taken. Tickets will be triaged to determine their mandate, severity and priority. If a Ticket is actioned, it becomes a File. For example;
    - a Ticket created from a low value Public Report will be assessed as low priority, and no further action will be taken – this Public Report would remain a Ticket.
    - A Public Report that is assessed and determined that it is linked to an ongoing intelligence File may be linked to that File by an Analyst.
    - A Submission that is received and assessed as high priority for action by the Operational Coordination Section will take on File status.
- **"TLP"** or **"Traffic Light Protocol"** means a set of designations that are used to ensure that sensitive information is shared with the appropriate audience (https://www.us-cert.gov/tlp). It employs four colours to indicate the expected sharing boundaries to be applied by the recipient(s):
    - **RED**: Non-disclosable information and distribution is restricted to personnel. The information can only be disseminated with an agreement from the data owner;
    - **AMBER**: Limited disclosure and restricted dissemination for official use only but not for publication or broadcast in a public venue;

  - **GREEN**: Information can be shared with others but not published or posted on the web; and
  - **WHITE**: Information that is for the public. Unrestricted dissemination (publication, web-posting or broadcast) and any member can publish the information (subject to copyright).
- **"TLS"** means Transport Layer Security are cryptographic protocols designed to provide communications security over a computer network.
- **"Topic Search"** or **"Subject Search"** or **"Descriptor Search"** means only the subject headings or descriptors are searched for words that match your search terms. Using subject headings ensures that all items about the same topic have consistent subject headings and so they can all be accessed with one search term.
- **"TRA"** means Threat and Risk Assessment that is a process of identifying system assets and how these assets can be compromised, assessing the level of risk that threats pose to assets, and recommending security measures to mitigate threats.
- **"TTP"** or **"Tactics, Techniques and Procedures"** means the behaviour of an actor. A tactic is the highest-level behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower level, highly detailed description on the context of a technique.
- **"TXT"** means a standard text document that contains unformatted text.
- **"UAT"** means User Acceptance Testing.
- **"Ubuntu"** is an Open source software operating system based on Debian Linux Distribution.
- **"UI"** or **"User Interface"** means the means by which the user and a computer system interact.
- **"URL"** means Uniform Resource Locator.
- **"User"** means an authorized person who uses the application.
- "User Access" means the rights given to a Client by the contractor to use the NCS solution as defined in the Statement of work in a Software as a Service (SaaS) distribution model.
- **"User Experience"** means an individual's reaction to the use of a particular product, system or service. It generally describes the emotional reaction to the use of the system mainly in light of its ease of use or the satisfaction it provides.
- **"VERIS"** or **"Vocabulary for Event Recording and Incident Sharing"** means a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner.
- **"VIP"** means Very Important Person.
- **"VPN"** means Virtual Private Network. It extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- **"W3C"** or **"World Wide Web Consortium"** is an international community where member organizations, a full-time staff, and the public work together to develop Web standards.
- **"Watch List"** means a list of indicators of compromise that can be used to identify cybercrime submissions of interest. A Watch list can contain observable type values (by example, IP Address, URL, Domain Name), Cybercrime Tools Techniques and Processes (TTP) (by example Trojan, programming language, key logger), Crime types (by example Ransomware, BEC, Crypto mining, Command and Control) or other identifying attributes of cybercrimes.
- **"WCAG"** means Web Content Accessibility Guidelines. It is developed through the W3C process in cooperation with individuals and organizations around the world, with a goal of providing a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally.
- **"WET"** means Web Experience Toolkit. It includes reusable components for building and maintaining innovative websites that are accessible, usable, and interoperable. These reusable components are open source software and free for use by GC departments and external Web communities.
- **"WORA"** or **"Write Once, Run Anywhere"** refers to a program's ability to run on all common operating systems.

- **“Workflow”** means the sequence of automated, manual, administrative, or other processes through which a piece of work passes from initiation to completion.
- **“XLSX”** means a Microsoft Excel file.
- **“XML”** means Extensible Markup Language that is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

ANNEX E

PRIVACY OBLIGATIONS

1. Auditing Compliance

(a) In the event Canada needs to conduct security audits, inspections and/or review any additional information (e.g., documentation, data protection description, data architecture and security descriptions) pursuant to Section 12.1, both Parties agree to negotiate a solution in good faith and consider both the rationale for Canada's request and the Contractor's processes and protocols.

(b) Within 30 days of request from the Contracting Authority, the Contractor must engage a third party to conduct a privacy audit or provide evidence to confirm that it does not generate, collect, use, store or disclose any additional personal information as defined by Canada, other than Client data as defined by the Contractor and does not specifically have Personal Information in Support Data (collected in logs (e.g., telemetry data such as email message headers and content).

2. Data Ownership and Privacy Requests

(a) Client Data including all Personal Information (PI) will be used or otherwise processed only to provide the Services, including purposes compatible with providing the Services. The Contractor must not use or otherwise process Canada Data or derive information from it for any advertising or similar commercial purposes. As between the parties, the Client retains all right, title and interest in and to Client Data. The Contractor acquires no rights in Canada Data, other than the rights Client grants to the Contractor to provide the Solution to the Customer.

(b) All data the Contractor stores, hosts or processes on behalf of Canada remains the property of Canada. When requested by the Contracting Authority, the Contractor must provide Personal Information records within five Federal Government Working Days (or seven Federal Government Working Days if it must be retrieved from offsite backup/replication) in a Word or Excel document.

3. Assist in Delivery of Canada's Privacy Impact Assessment

(a) Upon request of the Technical Authority, the Contractor must support Canada in creating a privacy impact assessment in accordance with the Treasury Board Directive on Privacy Impact Assessment (https://www.statcan.gc.ca/eng/about/pia/dcpia) by assisting the Canada with the supporting documentation including a foundational PIA for Canada provided by the Contractor. The Contractor agrees to provide this support within ten working days of a request or within a mutually agreed upon timeframe depending on the complexity of the request by the Canada.

4. Privacy Breach

(a) The Contractor must alert and promptly notify the Technical Authority (via phone and email) of any compromise, breach or of any evidence that leads the Contractor to reasonably believe that risk of compromise, or a breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365 days).

(b) If the Contractor becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data or Personal Information while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay:

(i) notify Canada of the Security Incident;

(ii) investigate the Security Incident and provide Canada with detailed information about the Security Incident; and

(iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(c) The Contractor must:

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

(ii) Tracks, or enables Canada to track, disclosures of Canada Data, including what data has been disclosed, to whom, and at what time.

ANNEX F

SUPPLY CHAIN INTEGRITY PROCESS

1. **Condition of Contract Award**: In order to be awarded a contract, the Bidder must successfully complete the Supply Chain Integrity Process ("SCI Process") and not be disqualified.

2. **Definitions**: The following words and expressions used with respect to SCI Process have the following meanings:

   a. **"Canada's Data"** means any data originating from the Work, any data received in contribution to the Work or any data that is generated as a result of the delivery of security, configuration, operations, administration and management services, together with any data that would be transported or stored by the contractor or any subcontractor as a result of performing the Work under any resulting contract;

   b. **"Product"** means any hardware that operates at the data link layer of the Open Systems Interconnection model (OSI Model) Layer 2 and above; any software; and any Workplace Technology Device;

   c. **"Product Manufacturer"** means the entity that assembles the component parts to manufacture the final Product;

   d. **"Software Publisher"** means the owner of the copyright of the software, who has the right to license (and authorize others to license/sub-license) its software products;

   e. **"Supply Chain Scope Diagram"**: A supply chain scope diagram is provided as Appendix M to provide a visual representation of the SCSI submission and assessment requirements described in further detail below. In the case of a discrepancy between the diagram and the process described in this document, this document will prevail;

   f. **"Supply Chain Security Information"** means any information that Canada requires a Bidder or Contractor to submit to conduct a complete security assessment of the SCSI as a part of the SCI process.

   g. **"Workplace Technology Device"** means any desktop, mobile workstation (such as a laptop or tablet), smart phone, or phone, as well as any peripheral item or accessory such as a monitor, keyboard, computer mouse, audio device or external or internal storage device such as a USB flash drive, memory card, external hard drive or writable CDs and DVDs or other media;

   h. **"Work"** means all the activities, services, goods, equipment, matters and things required to e done, delivered or performed by the contractor under any resulting contract;

3. **Bid Submission Requirements** (Mandatory at Bid Closing):
   Bidders must submit with their bids, by the closing date, the following Supply Chain Security Information ("SCSI"):

   a. **IT Product List**: Bidders must identify the Products over which Canada's Data would be transmitted and/or on which Canada's Data would be stored, or that would be used and/or installed by the Bidder or any of its subcontractors to perform any part of the Work, together with the following information regarding each Product:

      i. **Location**: identify where each Product is interconnected with any given network for Canada's Data (identify the service delivery points or nodes, such as points of presence, third party

locations, data centre facilities, operations centre, security operations centre, internet or other public network peering points, etc.);

ii. **Product Type**: identify the generally recognized description used by industry such as hardware, software, etc.; components of an assembled Product, such as module or card assembly, must be provided for all layer 3 internetworking devices;

IT Component: identify the generally recognized description used by industry such as firewall router, switch, server, security appliance, etc.;

iii. **Product Model Name or Number**: identify the advertised name or number of the Product assigned to it by the Product Manufacturer;

iv. **Description and Purpose of the Product**: identify the advertised description or purpose by the Product Manufacturer of the Product and the intended usage or role in the Work described for the Project;

v. **Source**: identify the Product Manufacturer and/or Software Publisher of embedded components;

vi. **Name of Subcontractor**: identify all subcontractors. In the "SCSI Submission Form" provided with this bid solicitation at Attachment 5.1, "Name of Subcontractor" refers to any subcontractor that will provide, install or maintain one or more Products, if the Bidder would not do so itself, as further defined below.

Submitting the information set out above is mandatory. Canada requests that bidders provide the IT Product List information by using the SCSI Submission Form, but the form in which the information is submitted is not itself mandatory. Canada also requests that, on each page, bidders indicate their legal name and insert a page number as well as the total number of pages. Canada further requests that Bidders insert a separate row in the SCSI Submission Form for each Product. Finally, Canada requests that Bidders not repeat multiple iterations of the same Product (e.g., if the serial number and/or the color is the only difference between two Products, they will be treated as the same Product for the purposes of the SCSI assessment).

b. **Network Diagrams**: one or more conceptual network diagrams that collectively show the complete network proposed to be used to perform the Work described in this bid solicitation. The network diagrams are only required to include portions of the Bidder's network (and its subcontractors' networks) over which Canada's Data would be transmitted in performing any resulting contract. As a minimum, the diagram must show:

i. the following key nodes for the delivery of the services under any resulting contract:
   1. service delivery points;
   2. core network; and
   3. subcontractor network(s) (specifying the name of the subcontractor as listed in the List of Subcontractors);

ii. the node interconnections, if applicable;

iii. any node connections with the Internet; and

iv. for each node, a cross-reference to the Product that will be deployed within that node, using the line item number from the IT Product List.

c. **List of Subcontractors**: The Bidder must provide a list of any subcontractors that could be used to perform any part of the Work (including subcontractors affiliated or otherwise related to the Bidder) pursuant to any resulting contract. The list must include at a minimum:
   i. the name of the subcontractor;

ii. the address of the subcontractor's headquarters;
iii. the portion of the Work that would be performed by the subcontractor; and
iv. the location(s) where the subcontractor would perform the Work.

This list must identify all third parties who may perform any part of the Work, whether they would be subcontractors to the Bidder, or subcontractors to subcontractors of the Bidder down the chain. This means that every subcontractor that could have access to Canada's Data or would be responsible either for transporting it or for storing it must be identified. Subcontractors would also include, for example, technicians who might be deployed to maintain the Bidder's solution. For the purposes of this requirement, a third party who is merely a supplier of goods to the Bidder, but who does not perform any portion of the Work, is not considered to be a subcontractor. If the Bidder does not plan to use any subcontractors to perform any part of the Work, Canada requests that the Bidder indicate this in its bid.

4. **Assessment of Supply Chain Security Information**:
   a. Canada will assess whether, in its opinion, the SCSI creates the possibility that the top-ranked Bidder's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information.

   b. In conducting its assessment:
      i. Canada may request from the Bidder any additional information that the Supply Chain Security Authority requires to conduct a complete security assessment of the SCSI. The Bidder will have 2 working days (or a longer period if specified in writing by Canada) to provide the necessary information to the Supply Chain Security Authority. Failure to meet this deadline will result in the bid being disqualified.

      ii. Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is included in the bid or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of the SCSI.

   c. If, in Canada's opinion, there is a possibility that any aspect of the SCSI, if used by Canada, could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information:

      i. Canada will notify the Bidder in writing (sent by email) and identify which aspect(s) of the SCSI is subject to concern(s) or cannot be assessed (for example, proposed future releases of products cannot be assessed). Any further information that Canada might be able to provide to the Bidder regarding its concerns will be determined based on the nature of the concerns. In some situations, for reasons of national security, it may not be possible for Canada to provide further information to the Bidder; therefore, in some circumstances, the Bidder will not know the underlying reasons for Canada's concerns with respect to a product, subcontractor or other aspect of the Bidder's SCSI. With respect to any concerns, Canada may, in its discretion, identify a potential mitigation measure that the Bidder would be required to implement with respect to any portion of the SCSI if awarded a contract.

      ii. The notice will provide the Bidder with a minimum of 3 opportunities to submit revised SCSI in order to address Canada's concerns. If Canada has identified a potential mitigation measure that the supplier would be required to implement if awarded a contract, the Respondent must confirm in its revised SCSI whether or not it agrees that any awarded contract will contain additional commitments relating to those mitigation conditions. The first revised SCSI must be submitted within the **10 calendar days** following the day on which Canada's written notification is sent to the Bidder (or a longer period specified in writing by the Supply Chain Security Authority). If concerns are identified by Canada regarding the first revised SCSI submitted after bid closing, the second revised SCSI must be submitted within **5 calendar days** (or a longer period specified in writing by the Supply Chain Security Authority). If concerns are identified by Canada regarding the second revised SCSI submitted after bid

closing, the third revised SCSI must be submitted within **3 calendar days** (or a longer period specified in writing by the Supply Chain Security Authority).

With respect to the revised SCSI submitted each time, the Bidder must indicate in its response whether the revision affects any aspect of its technical bid or certifications. The Bidder will not be permitted to change any price in its bid, but will be permitted to withdraw its bid if it does not wish to honour the pricing as a result of required revisions to the SCSI. Each time the Bidder submits revised SCSI within the allotted time, Canada will perform a further assessment of the revised SCSI and the following will apply:

1. If, in Canada's opinion, there is a possibility that any aspect of the Bidder's revised SCSI could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, the Bidder will be provided with the same type of notice described under paragraph 4.c), above. If, in Canada's opinion, the third post-bid-closing revised SCSI submission still raises concerns, any further opportunities to revise the SCSI will be entirely at the discretion of Canada and the bid may be disqualified by Canada at any time.

2. If the bid is not disqualified as a result of the assessment of the SCSI (as revised in accordance with the process set out above), after receiving the final revised SCSI, Canada will assess the impact of the collective revisions on the technical bid and certifications to determine whether they affect:
    a. the Bidder's compliance with the mandatory requirements of the solicitation;

    b. the Bidder's score under the rated requirements of the solicitation, if any; or

    c. the Bidder's ranking vis-à-vis other bidders in accordance with the evaluation process described in the solicitation.

3. If Canada determines that the Bidder remains compliant and that its ranking vis-à-vis other bidders has been unaffected by the revisions to the SCSI submitted after bid closing in accordance with the process described above, the Supply Chain Security Authority will recommend the top-ranked bid for contract award, subject to the provisions of the bid solicitation. If Canada's approval is subject to any mitigation measures, no contract will be awarded to the Respondent unless Canada is satisfied that the contract includes additional commitments reflecting the required mitigation measures.

4. If Canada determines that, as a result of the revisions to the SCSI submitted after bid closing in accordance with the process described above, the Bidder is either no longer compliant or is no longer the top-ranked bidder, Canada will proceed to consider the next-ranked bid for contract award, subject again to the provisions of the solicitation relating to the assessment of the SCSI submitted at bid closing, and to the assessment of any revised SCSI submitted after bid closing in accordance with the above provisions.

d. By participating in this process, the Bidder acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified. As a result:

    i. a satisfactory assessment does not mean that the same or similar SCSI will be assessed in the same way for future requirements; and

    ii. during the performance of any contract resulting from this bid solicitation, if Canada has concerns regarding certain products, designs or subcontractors originally included in the SCSI, the terms and conditions of that contract will govern the process for addressing those concerns.

5. By submitting its SCSI, and in consideration of the opportunity to participate in this procurement process, the Bidder agrees to the terms of the following non-disclosure agreement (the **"Non-Disclosure Agreement"**):

a. The Bidder agrees to keep confidential and store in a secure location any information it receives from Canada regarding Canada's assessment of the Bidder's SCSI (the **"Sensitive Information"**) including, but not limited to, which aspect of the SCSI is subject to concern, and the reasons for Canada's concerns.

b. Sensitive Information includes, but is not limited to, any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form or otherwise, and regardless of whether or not that information is labeled as classified, confidential, proprietary or sensitive.

c. The Bidder agrees that it will not reproduce, copy, divulge, release or disclose, in whole or in part, in whatever way or form any Sensitive Information to any person other than a person employed by the Bidder who has a need to know the information and has a security clearance commensurate with the level of Sensitive Information being disclosed, without first receiving the written consent of the Supply Chain Security Authority.

d. The Bidder agrees to notify the Supply Chain Security Authority immediately if any person, other than those permitted by the previous Sub-article, accesses the Sensitive Information at any time.

e. The Bidder agrees that a breach of this Non-Disclosure Agreement may result in disqualification of the Bidder at any stage of the procurement process, or immediate termination of a resulting contract or other resulting instrument. The Bidder also acknowledges that a breach of this Non-Disclosure Agreement may result in a review of the Bidder's security clearance and a review of the Bidder's status as an eligible bidder for other requirements.

f. All Sensitive Information will remain the property of Canada and must be returned to the Supply Chain Security Authority or destroyed, at the option of the Supply Chain Security Authority, if requested by the Supply Chain Security Authority, within 30 days following that request.

g. This Non-Disclosure Agreement remains in force indefinitely. If the Bidder wishes to be discharged from its obligations with respect to any records that include the Sensitive Information, the Bidder may return all the records to an appropriate representative of Canada together with a reference to this Non-Disclosure Agreement. In that case, all Sensitive Information known to the Bidder and its personnel (i.e., Sensitive Information that is known, but not committed to writing) would remain subject to this Non-Disclosure Agreement, but there would be no further obligations with respect to the secure storage of the records containing that Sensitive Information (unless the Bidder created new records containing the Sensitive Information). Canada may require that the Bidder provide written confirmation that all hard and soft copies of records that include Sensitive Information have been returned to Canada.

ANNEX G

TASK AUTHORIZATION FORM

TASK AUTHORIZATION (TA) FORM				
Contractor:		**Contract Number:**		
Commitment: #		**Financial Coding:**		
Task Number (Amendment):		**Issue Date:**	**Response Require By:**	
1. Statement of Work (Work Activities, Certifications and Deliverables)				
See attached for Statement of Work and Certifications required.				
2. Period of Service:	**From** (Date)		**To** (Date)	
3. Work Location:				
4. Travel Requirements:				
5. Language Requirement:				
6. Other Conditions/Constraints:				
7. Level of Security Clearance required for the Contractor Personnel:				
8. Contractor's Response:				

Category and Name of Proposed Resource	**PSPC Security File Number**	**Per Diem Rate**	**Estimated # of Days**	**Total Cost**
Estimated Cost				
Applicable Taxes				
Total Labour Cost				
Total Travel & Living Cost				

TASK AUTHORIZATION (TA) FORM	
Firm Price or Maximum TA Price	
Contractor's Signature	
Name, Title and Signature of Individual Authorized to sign on behalf of the **Contractor** (type or print) _____	Signature: _____ Date: _____
Approval – Signing Authority	
Signatures (Client) Name, Title and Signature of Individual Authorized to sign: Technical Authority: _____ Date: _____	**Signatures (PSPC)** Contracting Authority [1]: _____ Date: _____
[1] Signature required for TA valued at (*AMOUNT TO BE UPDATED AT CONTRACT AWARD)* or more, Applicable Taxes included.	
You are requested to sell to her Majesty the Queen in Right of Canada, in accordance with the terms and conditions set out herein, referred to herein, or attached hereto, the services listed herein and in any attached sheets at the price set out thereof.	

APPENDIX A TO ANNEX G

CERTIFICATIONS AT THE TASK AUTHORIZATION STAGE

The following Certifications are to be used, as applicable. If they apply, they must be signed and attached to the Contractor's quotation when it is submitted to Canada.

1. CERTIFICATION OF EDUCATION AND EXPERIENCE

The Contractor certifies that all the information provided in the résumés and supporting material proposed for completing the subject work, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Contractor to be true and accurate. Furthermore, the Contractor warrants that every individual proposed by the Contractor for the requirement is capable of performing the Work described in the Task Authorization.

_____ _____

Print name of authorized individual & sign above Date

2. CERTIFICATION OF AVAILABILITY OF PERSONNEL

The Contractor certifies that, should it be authorized to provide services under this Task Authorization, the persons proposed in the quotation will be available to commence performance of the work within a reasonable time from the date of issuance of the valid Task Authorization, or within the time specified in the TA Form, and will remain available to perform the work in relation to the fulfillment of the requirement.

_____ _____

Print name of authorized individual & sign above Date

3. CERTIFICATION OF STATUS OF PERSONNEL

If the Contractor has proposed any individual who is not an employee of the Contractor, the Contractor certifies that it has permission from that individual to propose his/her services in relation to the Work to be performed under this TA and to submit his/her résumé to Canada. At any time during the Contract the Contractor must, upon request from the Contracting Authority, provide the written confirmation, signed by the individual, of the permission that was given to the Contractor of his/her availability. Failure to comply with the request may result in a default under the Contract in accordance with the General Conditions.

_____ _____

Print name of authorized individual & sign above Date

4. CERTIFICATION OF LANGUAGE

The Contractor certifies that the proposed resource(s) in response to this draft Task Authorization is/are fluent in English. The individual(s) proposed must be able to communicate orally and in writing in English without any assistance and with minimal errors.

_____ _____

Print name of authorized individual & sign above Date

ANNEX H

PROGRESS CLAIMS

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

Claim for Progress Payment
Demande de paiement progressif

If necessary, use form PWGSC-TPSGC 1112 to record detail costs
Si nécessaire, utiliser le formulaire PWGSC-TPSGC 1112 pour inscrire les coûts détaillés

Contractor's Name and Address Nom et adresse de l'entrepreneur	Claim No. N° de la demande	Date YYYY-MM-DD / AAAA-MM-JJ	Contract Price - Prix contractuel
	File No. - N° du dossier		Contract Serial No. N° de série du contrat

Contractor's Procurement Business Number (PBN) Numéro d'entreprise-approvisionnement (NEA) de l'entrepreneur	Financial Code(s) - Code(s) financier(s)

Contractor's Report of Work Progress (if needed, use additional sheets)
Compte rendu de l'avancement des travaux par l'entrepreneur (si nécessaire, utiliser des feuilles supplémentaires)

Period of work covered by the claim
Période des travaux visée par la demande ▶

Description: (Expenditures must be claimed in accordance with the basis and/or method of payment of the contract) **Description** : (Les dépenses doivent être réclamées conformément à la base de paiement et (ou) à la méthode de paiement du contrat).	Current Claim Demande courante (A) ☐ 3 decimal	Tax Rate Taux de taxe	Previous Claims Demandes précédentes (B) ☐ 3 decimal	Tax Rate Taux de taxe	Total to Date Total à date (A + B)
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	
		%		%	

Contractor's GST No. N° de TPS de l'entrepreneur	Subtotal Sous-total			
Contractor's QST No. No. de TVQ de l'entrepreneur	Applicable taxes Taxes applicables			
	Total			
	Less holdbacks on expenditures only (Applicable taxes excluded) Moins les retenues sur les dépenses uniquement (Taxes applicables en sus)			

Total Amount of Claim (including applicable taxes)
Montant total de la demande (incluant les taxes applicables)

Percentage of the work completed Pourcentage des travaux achevés	%	Current Claim Demande courante ▶	Amount due Montant dû

Canada

Claim No. N° de la demande	Contract Serial No. N° de série du contrat

CERTIFICATE OF CONTRACTOR

I certify that:

- All authorizations required under the contract have been obtained. The claim is consistent with the progress of the work and is in accordance with the contract.
- Indirect costs have been paid for or accrued in the accounts.
- Direct materials and the subcontracted work have been received, accepted and either paid for or accrued in the accounts following receipt of invoice from supplier/subcontractor, and have been or will be used exclusively for the purpose of the contract.
- All direct labour costs have been paid for or accrued in the accounts and all such costs were incurred exclusively for the purpose of the contract;
- All other direct costs have been paid for or accrued in the accounts following receipt of applicable invoice or expense voucher and all such costs were incurred exclusively for the purpose of the contract; and
- No liens, encumbrances, charges or other claims exist against the work except those which may arise by operation of law such as a lien in the nature of an unpaid contractor's lien and in respect of which a progress payment and/or advance payment has been or will be made by Canada.

ATTESTATION DE L'ENTREPRENEUR

J'atteste que :

- Toutes les autorisations exigées en vertu du contrat ont été obtenues. La demande correspond à l'avancement des travaux et est conforme au contrat.
- Les coûts indirects ont été réglés ou portés aux livres.
- Les matières directes et les travaux de sous-traitance ont été reçus, et le tout a été accepté et payé, ou encore porté aux livres après réception de factures envoyées par le fournisseur ou le sous-traitant; ces matières et ces travaux ont été ou seront utilisés exclusivement aux fins du contrat.
- Tous les coûts de la main-d'oeuvre directe ont été réglés ou portés aux livres et tous ces coûts ont été engagés exclusivement aux fins du contrat.
- Tous les autres coûts indirects ont été réglés ou portés aux livres après réception des factures ou pièces justificatives pertinentes et tous ces coûts ont été engagés exclusivement aux fins du contrat.
- Il n'existe aucun privilège ni demande ou imputation à l'égard de ces travaux sauf ceux qui pourraient survenir par effet de la loi, notamment le privilège d'un entrepreneur non payé à l'égard duquel un paiement progressif et(ou) un paiement anticipé a été ou sera effectué par le Canada.

Contractor 's Signature - Signature de l'entrepreneur	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

Check the box if the claim is being made with respect to advance payment provisions included in the basis of payment of the contract. ☐

Cocher la case si la demande est faite en rapport avec les dispositions relatives aux paiements anticipés qui se trouvent dans la base de paiement du contrat.

This claim, or a portion of this claim, is for an advance payment.

Cette demande, ou une partie de cette demande, est pour un paiement anticipé.

I certify that:

- The funds received will be used solely for the purpose of the contract and attached is a complete description of the purpose to which the advance payment will be applied.
- The amount of the payment is established in accordance with the conditions of the contract.
- The contractor is not in default of its obligations under the contract.
- The payment is related to an identifiable part of the contractual work.

J'atteste que :

- Les fonds reçus ne serviront uniquement qu'aux fins du contrat; ci-joint est une description complète des fins auxquelles le paiement anticipé sera utilisé.
- Le montant du paiement est établi conformément aux conditions du contrat.
- L'entrepreneur n'a pas manqué à ses obligations en vertu du contrat.
- Le paiement porte sur une partie identifiable des travaux précisés dans le contrat.

Contractor 's Signature - Signature de l'entrepreneur	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

CERTIFICATES OF DEPARTMENTAL REPRESENTATIVES

Scientific/Project/Inspection Authority: I certify that the work meets the quality standards required under the contract, and its progress is in accordance with the conditions of the contract.

Inspection Authority (all other contracts): I certify that the quality of the work performed is in accordance with the standards required under the contract.

ATTESTATIONS DES REPRÉSENTANTS DU MINISTÈRE

Autorité scientifique ou responsable du projet / de l'inspection : J'atteste que les travaux sont conformes aux normes de qualité exigées en vertu du contrat et que leur avancement est conforme aux conditions du contrat.

Responsable de l'inspection (tous les autres contrats) : J'atteste que la qualité des travaux exécutés est conforme aux normes exigées en vertu du contrat.

Signature of Scientific / Project / Inspection Authority Signature de l'autorité scientifique ou responsable du projet / de l'inspection	Date (YYYY-MM-DD / AAAA-MM-JJ)

PWGSC Contracting Authority: I certify that, to the best of my knowledge, the claim is consistent with the progress of the work and is in accordance with the contract. This claim, however, may be subject to further verification and any necessary adjustment before final settlement.

Autorité contractante de TPSGC : J'atteste, au meilleur de ma connaissance, que la demande correspond à l'avancement des travaux et est conforme au contrat. Toutefois, cette demande pourrait faire l'objet d'une autre vérification et de tout rajustement nécessaire avant le règlement final.z

Contracting Authority Signature de l'autorité contractante	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

Client's Authorized Signing Officer - (must sign the interim claim): I certify that the claim is in accordance with the contract.

Signataire autorisé du client - (doit signer la demande provisoire) : J'atteste que la demande est conforme au contrat.

Client Signature du client	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

Client's Authorized Signing Officer - (must sign the final claim): I certify that all goods have been received and all services have been rendered, that the work has been properly performed and that the claim is in accordance with the contract.

Signataire autorisé du client - (doit signer la demande finale) : J'atteste que tous les biens ont été reçus, que tous les services ont été rendus, que tous les travaux ont été exécutés convenablement, et que la demande est conforme au contrat.

Client Signature du client	Title - Titre	Date (YYYY-MM-DD / AAAA-MM-JJ)

ANNEX I

BIDDER FORMS

FORM 1 – BIDDER'S FORMS

BID SUBMISSION FORM		
Bidder's full legal name ***[Note to Bidders:** Bidders who are part of a corporate group should take care to identify the correct corporation as the Bidder.]*		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	Name:	
	Title:	
	Address:	
	Telephone #:	
	Fax #:	
	Email:	
Bidder's Procurement Business Number (PBN) *[see the Standard Instructions 2003]* [***Note to Bidders:** Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]*		
Jurisdiction of Contract: Province or Territory in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
Former Public Servants See the Article in Part 2 of the bid solicitation entitled "Former Public Servant" for a definition of "Former Public Servant".	Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant "	

BID SUBMISSION FORM

	Is the Bidder a FPS who received a lump sum payment under the terms of the terms of the Work Force Adjustment Directive? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant "	
Canadian Content Certification As described in the solicitation, bids with at least 80% Canadian content are being given a preference. *[For the definition of Canadian goods and services, consult the PWGSC SACC clause A3050T]*	On behalf of the Bidder, by signing below, I confirm that *[check the box that applies]:*	
	At least 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)	
	Less than 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)	
Hardware: *(Contracting Authority should only insert when Supplemental General Conditions 4001 have been inserted in Part 7).*	Toll-Free Telephone Number for maintenance services:	
	Website for maintenance services:	
Licensed Software Maintenance and Support: *(Contracting Authority should only insert when supplemental General Conditions 4004 has been inserted in Part 7).*	Toll-free Telephone Access:	
	Toll-Free Fax Access:	
	E-Mail Access:	
	Website address for web support:	
Security Clearance Level of Bidder **[include both the level and the date it was granted]** [**Note to Bidders:** *Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security clearance is not valid for the Bidder.]*		

On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that:

1. The Bidder considers itself and its products able to meet all the mandatory requirements described in the bid solicitation;
2. This bid is valid for the period requested in the bid solicitation;
3. All the information provided in the bid is complete, true and accurate; and
4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.

BID SUBMISSION FORM	
Signature of Authorized Representative of Bidder	_____

FORM 2 - CLOUD SERVICE PROVIDER LETTER OF ATTESTATION

Name of Respondent _____

This authorization applies to the following proposed Commercially Available Public Cloud Service (Name of the Propose solution):

_____

The Respondent declares that is underlaying infrastructure and platforms is hosted on a Commercially Available Public Cloud Services:

The definition of "Cloud Service Provider" for the purposes of this certification can be found in Annex D – Definitions and Interpretations of the Request for Proposal.

Cloud Service Provider _____

Cloud Service Provider Data Center Location _____

Signature of authorized signatory of CSP _____

Print Name of authorized signatory of CSP _____

Print Title of authorized signatory of CSP _____

Address for authorized signatory of CSP _____

Telephone no. for authorized signatory of CSP _____

Fax no. for authorized signatory of CSP _____

Date signed _____

FORM 3 – SOFTWARE PUBLISHER CERTIFICATION FORM

Form 3 **Software Publisher Certification Form** (to be used where the Bidder itself is the Software Publisher)
The Bidder certifies that it is the software publisher of all the following software products and that it has all the rights necessary to license them (and any non-proprietary sub-components incorporated into the software) on a royalty-free basis to Canada pursuant to the terms set out in the resulting contract:
[Bidders should add or remove lines as needed]

FORM 4 – SOFTWARE PUBLISHER AUTHORIZATION FORM

Form 4
Software Publisher Authorization Form
(to be used where the Bidder is not the Software Publisher)

This confirms that the software publisher identified below has authorized the Bidder named below to license its proprietary software products under the contract resulting from the bid solicitation identified below. The software publisher acknowledges that no shrink-wrap or click-wrap or other terms and conditions will apply, and that the contract resulting from the bid solicitation (as amended from time to time by its parties) will represent the entire agreement, including with respect to the license of the software products of the software publisher listed below. The software publisher further acknowledges that, if the method of delivery (such as download) requires a user to "click through" or otherwise acknowledge the application of terms and conditions not included in the bid solicitation, those terms and conditions do not apply to Canada's use of the software products of the software publisher listed below, despite the user clicking "I accept" or signalling in any other way agreement with the additional terms and conditions.

This authorization applies to the following software products:

_____

_____

[Bidders should add or remove lines as needed]

Name of Software Publisher (SP) _____

Signature of authorized signatory of SP _____

Print Name of authorized signatory of SP _____

Print Title of authorized signatory of SP _____

Address for authorized signatory of SP _____

Telephone no. for authorized signatory of SP _____

Fax no. for authorized signatory of SP _____

Date signed _____

Solicitation Number _____

Name of Bidder _____

FORM 5 - DECLARATION FORM

This declaration form must be submitted as part of the bidding process. Please complete and submit in a **sealed envelope labelled "Protected"** to the attention of Integrity, Departmental Oversight Branch, PWGSC, 11 Laurier Street, Place du Portage, Phase III, Tower A, 10A1, Room 108, Gatineau (Québec) Canada K1A 0S5. Include the sealed envelope with your bid submission. This form is considered "Protected B" when completed.	
Complete Legal Name of Company:	
Company's address:	
Company's Procurement Business Number (PBN):	
Bid Number:	
Date of Bid: (YY-MM-DD)	

Have you ever, as the bidder, your affiliates or as one of your directors, been convicted or have pleaded guilty of an offence in Canada or similar offence elsewhere under any of the following provisions [1]:			
	Yes	**No**	**Comments**
Financial Administration Act 80(1) d): False entry, certificate or return 80(2): Fraud against Her Majesty 154.01: Fraud against Her Majesty **Criminal Code** 121: Frauds on the government and contractor subscribing to election fund 124: Selling or Purchasing Office 380: Fraud – committed against Her Majesty 418: Selling defective stores to Her Majesty	☐	☐	
In the last 3 years, have you, as the bidder, your affiliates or one of your directors, been convicted or have pleaded guilty of an offence in Canada or elsewhere under any of the following provisions [1]:			
Criminal Code 119: Bribery of judicial officers,... 120: Bribery of officers 346: Extortion 366 to 368: Forgery and other offences resembling forgery 382: Fraudulent manipulation of stock exchange transactions 382.1: Prohibited insider trading 397: Falsification of books and documents 422: Criminal breach of Contract 426: Secret commissions 462.31 Laundering proceeds of crime 467.11 to 467.13: Participation in activities of criminal organization **Competition Act** 45: Conspiracies, agreements or arrangements between competitors 46: Foreign directives 47: Bid rigging 49: Agreements or arrangements of federal financial institutions	☐	☐	

[1] for which no pardon or equivalent has been received.

	Yes	No	Comments
52: False or misleading representation 53: deceptive notice of winning a prize			
Corruption of Foreign Public Officials Act 3: Bribing a foreign public official 4: Accounting 5: Offence committed outside Canada **Controlled Drugs and Substance Act** 5: Trafficking in substance 6: Importing and exporting 7: Production of substance	☐ ☐	☐ ☐	
Other Acts 239: False or deceptive statements of the Income Tax Act 327: False or deceptive statements of the Excise Tax Act	☐	☐	

Additional Comment

☐ I, (name)_____, (position)_____, of (company name bidder)_____ _____authorise PWGSC to collect and use the information provided, in additional to any other information that may be required to make a determination of ineligibility and to publicly disseminate the results.

☐ I, (name) _____, (position) _____, of (company name bidder)_____certify that the information provided in this form is, to the best of my knowledge, true and complete. Moreover, I am aware that any erroneous or missing information could result in the cancellation of my bid as well as a determination of ineligibility/suspension.

We appreciate your interest in doing business with The Government of Canada and your understanding on the additional steps that we need to take to protect the integrity of PWGSC's procurement process.

FORM 6 - LIST OF NAMES FORM

In accordance with Part 5, Article 5.3, – Integrity Provision – List of Names, please complete the Form below.

Complete Legal Name of Company	
Company's address	
Company's Procurement Business Number (PBN)	
Solicitation number	
Board of Directors (Use Format – first name last name) Or put the list as an attachment	
1. Director	
2. Director	
3. Director	
4. Director	
5. Director	
6. Director	
7. Director	
8. Director	
9. Director	
10. Director	
Other members	
Comments	

Form 7 to Part 5 – Bid Solicitation (*insert if applicable*)
FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY – CERTIFICATION

Remark to Contracting Authority: *Insert the following certification for requirements issued on behalf of a Department or Agency subject to the FCP, estimated at $1,000,000* ***and above****, options excluded and Applicable Taxes included: (consult Annex 5.1 of the Supply Manual)(See also Part 5 - Certifications and Part 7 - Resulting Contract Clauses)*

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with any request or requirement imposed by Canada may render the bid non-responsive or constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment and Social Development Canada (ESDC) - Labours' website.

Date:_____(YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the *Employment Equity Act.*

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 employees (combined work force includes: permanent full-time, permanent part-time and temporary employees [temporary employees only includes those who have worked 12 weeks or more during a calendar year and who are not full-time students]).

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1 The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with ESDC -Labour.

OR

( ) A5.2. The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC -Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to ESDC - Labour.

B. Check only one of the following:

( ) B1 The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions).

FORM 8 - ELECTRONIC PAYMENT INSTRUMENTS

As indicated in Part 3, clause 3.1.2, the Bidder must identify which electronic payment instruments they are willing to accept for payment of invoices.

The Bidder accepts any of the following Electronic Payment Instrument(s):

( ) VISA Acquisition Card;

( ) MasterCard Acquisition Card;

( ) Direct Deposit (Domestic and International);

( ) Electronic Data Interchange (EDI);

( ) Wire Transfer (International Only);

( ) Large Value Transfer System (LVTS) (Over $25M)

FORM 9 - Financial Bid Presentation Sheet

Bidders must use Annex B- Basis of Payment Pricing Tables to complete their Financial bid Response.

All prices must be provided in Canadian dollars exclusive of any applicable taxes.

ANNEX J

TECHNICAL EVALUATION

BID EVALUATION CRITERIA

1. This document contains the Mandatory technical criteria and Point Rated Criteria that will be used to evaluate a Bidder's technical proposal for the *National Cybercrime Solution*.

2. Bidders should provide a complete technical and functional specification proposal describing in detail how they meet each of the criteria. The Bidder should provide a reference to the proposal page number for each criteria to be addressed.

1.0 Mandatory Criteria (MC)

This section specifies Bidder qualifications that must be met as well as functional requirements that the Solution must be able to provide.

For each mandatory requirement, please include a reference to the appropriate page in your proposal that responds to the requirement. To be considered responsive, all mandatory criteria must be met. Subject to the Phased Bid Compliance Process, Proposals that fail to meet the mandatory requirements are given no further consideration.

1.1 BACKGROUND AND CORPORATE QUALIFICATIONS MANDATORY CRITERIA

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
Background and Corporate Experience				
MC-1	**Corporate Experience** The Bidder must demonstrate that it has the corporate qualifications and experience to deliver the Solution and the resource capacity to execute the configuration, integration, testing, implementation and support work after contract award by providing the following information: a) An overview of the Bidder corporate organization including at a minimum: i. A description of its corporate structure; ii. The number of years in business; iii. An overview of main business activities; iv. Examples of major customers; v. A recent estimate of the number of employees; and, vi. An overview of geographic presence (locations). b) A corporate history in relation to software products, designed to help law enforcement or government agencies through analysis and operational coordination across multiple jurisdictions. c) A description of the Bidder's relationship and experience with the software products being proposed.			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	d) An overview of the Bidder's knowledge and experience in the delivery of solutions similar in scope and complexity as NCS.			
MC-2	**Corporate Project References** The Bidder must demonstrate its experience executing three (3) contracts for government or private sector agencies that involve configuring, implementing and supporting solutions similar in scope and size to the NCS. Of the 3 contracts provided as project reference, the Bidder must include one contract where they have provided a software solution, designed to help law enforcement or government agencies through analysis, case management and operational and intelligence coordination across multiple jurisdictions. To demonstrate this experience, the bidder must provide, for each reference contract, the following information: a) A description of the client's organization; b) The client contact name, information (email address and phone number); c) The start and end dates of the contract; d) The contract value in Canadian dollars; e) A brief description of the scope of work and the outcomes of the contract; f) The month/year the end-product was deployed; g) The size of team provided by the Bidder; h) The status, (for example; completed, cancelled or in progress); i) The approximate size of the user community; j) Whether or not the user community is currently using the product; k) A brief description of the project activities related to Installation, Testing, Deployment, Integration, Configuration, Training and on-going Support; and, l) Other information that the Bidder deems appropriate, with a clear indication as to its pertinence.			
MC-3	**Senior Contractor Project Manager**			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	The Bidder must identify a Senior Contractor Project Manager (CPM) to be the single point of contact for all aspects of the contract execution work. A. The Senior CPM must have a minimum of Ten (10) years (as of the solicitation closing date of issuance of this solicitation) experience as a Senior Project Manager or Project Executive on IM/IT projects. B. The Bidder must also provide for the candidate, a description of three (3) major projects that the candidate has delivered over the last Ten (10) years. For each referenced project, the Bidder must provide: a) Project name. b) Project value. c) Project duration. d) Start and end dates of candidate involvement on the project. e) Candidate client contact information (for example; name, title, organization, email address and phone number). f) Role of the candidate on the project. The resume for the proposed Senior CPM must be provided with the bid.			

3.2 FUNCTIONAL REQUIREMENTS MANDATORY CRITERIA

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
Functional Requirements				
Case Management				
Ticket Management				
MC-4	The Bidder's proposed Solution must support automatic creation of Tickets for all Submissions and Service Requests received via Police and Partner Portal, Public Portal and Email including: a. Monitoring multiple email addresses for incoming Submissions and Service Requests			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	b. Parsing of contents, metadata and Indicators of Compromise from Submissions, Service Requests and attachments c. Automatic creation of a hash value of each email and attachment d. Assignment of a unique reference number to each Ticket			
Triage and Assessment				
MC-5	The Bidder's proposed Solution must automatically correlate Ticket data to existing data in the NCS Data Repository, store linkages and notify implicated Users, Groups, Agencies or Cybercrime Partners based on correlation results.			
MC-6	The Bidder's proposed Solution must use configurable business rules to determine severity and priority and automatically route Tickets for further processing.			
Work Queues				
MC-7	The Bidder's proposed Solution must support the following Work Queue functionality: a. User access to their Tasks and Work Items b. Referral of Tasks and Work items to users or groups c. Assignment of Tasks and Work Items to users or groups d. Search, Filter and Sort on multiple Task or Work Item attributes e. Progress Tracking on work items and tasks			
Ticket, File and Project Management				
MC-8	The Bidder's proposed Solution must support management of Tickets, Files and Projects including: a. User Creation b. Validation c. Routing d. Search e. View f. Print			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	g. Modification h. Merge/Un-Merge i. Split j. Link, unlink and view Attachments k. Link and un-link Tickets, Files and Projects l. Manage Tasks m. Manage Status n. Manage History o. Referral; to NC3 Sections or external Partners p. Cancel			
MC-9	The Bidder's proposed Solution must uniquely identify each File and Project with an Identification Number.			
MC-10	The Bidder's proposed Solution must allow a user to create a printable "Disclosure Package" containing all contents and activities related to a File or Project including all Submission, Ticket and File Data, Metadata, Activity Logs, System Audit Logs and Attachments, allowing for changes to configuration, content and layout.			
MC-11	The Bidder's proposed Solution must, for all Tickets, Files and Projects, include the following packaging and printing functionality: a. Allow a user to print any or all contents to printer or electronic file copy (for example; .pdf) b. Allow a user to create a hash value of any report or attachment and share the hash value along with the applicable report or attachment c. Automatically apply configurable information security designation and sharing protocol watermarks to outputs based on the printed data and allow a user to override or apply watermarks manually			
Police and Partner Portal (P3)				

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
MC-12	The Bidder's proposed Solution must include a Portal that will provide authorized external partners and Law Enforcement Agencies with a secure means of system access including: a. Search of the NCS Data Repository b. Submit Cybercrime Submissions and Service Requests to the NC3 or to other P3 Agencies c. Receive and Manage Notifications, Referrals, Messages and Requests			
MC-13	The Bidder's proposed Solution must allow a P3 User to manage local configurations and preferences including: a. Watchlists b. Public Reporting File Viewing Filters c. Notification Options d. Contact Information			
Functional Services				
Notifications				
MC-14	The Bidder's proposed Solution must support automatic real-time Notifications ("Alerts") to implicated users and groups using email and the Police and Partner Portal (P3).			
MC-15	The Bidder's proposed Solution must provide Users with the ability to create and send Notifications and Requests to Users and Groups.			
Dashboards				
MC-16	The Bidder's proposed Solution must provide configurable Dashboards allowing access to Notifications, messages, assigned work items and tasks and graphical views of situational awareness and operational reports.			
Data Analytics				

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
MC-17	The Bidder's proposed Solution must provide automated capabilities to analyse data to identify trends, groupings, and linkages and produce and share data visualization outputs including link charts, graphs and geospatial maps.			
MC-18	The Bidder's proposed Solution must allow a user to redact (Block-out or withhold non-disclosable) information in an output without removing the information from the original record.			
Configuration and Administration				
MC-19	The Bidder's proposed Solution must allow an authorized user to manage: a. Content of data validation and pick-list tables b. Partner and client profile information c. Templates; Data Entry and Notification d. Workflow Rules			
NCS Repository Query				
MC-20	The Bidder's proposed Solution must provide the ability to perform a federated search of all NCS Data Repository contents, structured and unstructured, including relational or non-relational databases, Data Catalogs and Object Stores.			
MC-21	The Bidder's proposed Solution must be able of triggering Notifications to implicated parties based on NCS Repository query correlations including; a. Querying data submitted by another agency b. Querying data that is on a Watchlist or "Be on Lookout" (BOLO) c. Querying data that has been queried by another agency			
Maintain Business Rules and Watchlists				
MC-22	The Bidder's proposed Solution must support the management of configurable business rules used to: a. Determine severity scores related to Submissions			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	b. Determine work priorities of Service Requests and Submissions c. Identify and prioritize submissions of interest based on needs of various sections within the NC3 d. Establish Watchlists			
Cyber Toolbox / Knowledgebase Service				
MC-23	The Bidder's proposed Solution must support the management of partner requests to access cybercrime forensic applications and services provided by NC3.			
Artificial Intelligence, Machine Learning and Natural Language Processing				
MC-24	The Bidder's proposed Solution must be able of using Natural Language Processing to extract text and content from unstructured data (unstructured text and images).			
MC-25	The Bidder's proposed Solution must be able of converting: a. English/French and non-English/French Language Audio to English text b. English text to French text and French text to English text c. Non-English Language text to English text			
MC-26	The Bidder's proposed Solution must support processes to monitor the outcomes of Artificial Intelligence to verify compliance with Government of Canada Directive on Automated Decision making and override unintentional outcomes as necessary.			
Business Intelligence Reporting				
MC-27	The Bidder's proposed Solution must allow authorized users to generate real-time reports from their desktop including: a. Pre-defined reports based on report criteria b. Ad hoc reports			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	c. Audit reports d. Ability to save reports for future execution e. Ability to save and share report results			
Cross-Reference Malware				
MC-28	The Bidder's proposed Solution must support the management of Malware Cross-Reference Requests including: a. Receiving requests and safely storing Malware Samples b. Correlating requests and samples against NCS Data Holdings c. Forwarding samples to selected external Malware Analysis Services, and d. Receiving, storing and forwarding malware analysis reports to requesters			
Automated Enrichment				
MC-29	The Bidder's proposed Solution must be able of automatically linking entities based on common attributes, while also including the ability to review linked entities and separate linkages as required. The Solution must also trigger Notifications based on linkages to support de-confliction.			
Technical Requirements				
Speech to Text, Translation and Optical Character Recognition				
MC-30	The Bidder's proposed Solution must provide a means of converting audio to text as well as images of printed or handwritten text into machine usable data.			
Identity Management				
MC-31	The Bidder's proposed Solution must demonstrate support for login (Authentication) functionality for all users (including P3) that adheres to the Government of Canada			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	Directive on User Authentication Guidance for Information Technology Systems ITSP.30.031 V2.			
MC-32	The Bidder's proposed Solution must be capable of using the RCMP tenant's Azure Active Directory for Authentication and Identity Management.			
MC-33	The Bidder's proposed Solution must provide Single Sign-On/Single Log-Out functionality for all internal users. External Partners (P3 users) are not subject to Single Sign-On/Off.			
Submission Quarantine				
MC-34	The Bidder's proposed Solution must include the ability to identify and store separately, all Submissions and Requests (including attachments) that contain malicious content.			
Secure Information Transfer				
MC-35	The Bidder's proposed Solution must be capable of securely exchanging encrypted content via email and the Police and Partner Portal.			
Data Import/Export Capability				
MC-36	The Bidder's proposed Solution must be capable of importing, exporting, decompressing and compressing data including support for the secure exchange of large files (files larger than 1 terabyte).			
Data Exchange Standards				
MC-37	The Bidder's proposed Solution must be able of data-sharing with the Malware Information Sharing Platform (MISP).			
Information Management				
MC-38	The Bidder's proposed Solution must support management and document marking using configurable information sharing protocols and data security designations including: a. Traffic Light Protocol			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	b. Government of Canada Information Security designations c. Europol information Handling Codes			
MC-39	The Bidder's proposed Solution must support the following Information Lifecycle Management (ILM) capabilities: a. Manage data retention per configurable retention and disposition schedules and Dates b. Protect information and data from accidental loss and corruption c. Protect information from unauthorized access d. Permit access to information to Groups and User Roles based on assigned roles and data attributes (RBAC and ABAC) e. Support automatic and manual purging of data f. Mark information as sequestered g. Trigger review, re-labelling, exporting and purging information that has exceeded security level of Protected B h. Support Data Residency in Canada			
Role Based Access Control and Attribute Based Access Controls				
MC-40	The Bidder's proposed Solution must support the use of configurable Role Based Access Controls (RBAC) and Attribute Based Access Controls (ABAC) to limit access to functionality and data.			
Integration				
MC-41	The Bidder's proposed Solution must support integration with the RCMPs enterprise email system in order to ingest as well as send submissions and service requests.			
MC-42	The Bidder's proposed Solution must support ingestion of Public Reports from the National Cybercrime and Fraud Reporting System (NCFRS) via a data feed.			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
MC-43	The Bidder's proposed Solution must support integration with Esri GIS to manage, analyze and share geospatial data.			
Activity and Audit Logging				
MC-44	The Bidder's proposed Solution must have the ability to create and maintain immutable activity logs and audit logs of all user and system activities including: • Adding, modifying and deleting data • Printing and exporting data • Query parameters and result sets • System processes • User system access • Viewing of logs per Role and Attribute Based Access • Containing minimally; User ID or System ID, Timestamp and Activity			
On-Line Text Chat				
MC-45	The Bidder's proposed Solution must support and manage secure on-line text chat communications between Users.			
Document Publishing and Productivity				
MC-46	The Bidder's proposed Solution must support Application Associations to provide seamless open, launch, view and edit capabilities related to attached files including MS Office document and spreadsheet and Adobe PDF.			
Usability				
MC-47	The Bidder must describe how its Solution conforms to applicable Government of Canada IT system usability standards for accessibility and common look and feel, which are derived from the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0 Standards.			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	Refer to https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32620.			
MC-48	The Bidder's Solution must include a plan to provide a 100% bilingual (French and English) Solution on all platforms offered in accordance with Government of Canada Policy on Official Languages. This means users selecting French as their language will not see anything in English in the solution's GUI, including but not limited to help files, tutorials, error messages and legal information. (User-generated content is excluded). The Bidder must also demonstrate how it regularly provides on-going support and maintenance services, as well as help desk support in English and French. Refer to https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26160&section=html			
MC-49	The Bidder's proposed Solution must support User configurable: a. Business Rules b. Data Entry and Query Templates c. Data Selection Lists d. Dashboards			
NCS Data Repository				
MC-50	The Bidder's proposed Solution must support a Cloud based elastic and scalable centralized Data Repository.			
Non-Functional				
MC-51	The Bidder's proposed Solution must be designed to be operational in a High Availability environment (available 99.45% averaged over a month).			
MC-52	The Bidder's proposed Solution must be able to accept changes in size and volumes with minimum effort while retaining acceptable performance levels. The changes may be in the form of (but not limited to) one or more of: a. additional concurrent users			

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
	b. additional geographic locations c. additional partner organizations d. additional functionalities e. additional volumes f. additional concurrent processes			
MC-53	The Bidder's proposed Solution must support a minimum of 500 concurrent users with no degradation in performance.			
MC-54	The Bidder's proposed Solution must provide users with the ability to manage their password in compliance with RCMP standards including: a. Mandatory password for all users b. Password contains a minimum of 8 characters including a mix of uppercase & lowercase and at least one special character c. Password change must be enforced at first new user login or issuance of new temporary password d. Periodic Password change must be enforced e. Users must have the ability to change their password at any time			
Cloud Service Provider SCED Compliance				
MC-55	The Bidder's proposed Solution must be deployable on a cloud platform that has been successfully onboarded to SSC/TBS's SCED (Secure Cloud Enablement and Defence) project. The Bidder must demonstrate compliance by providing evidence confirming successful integration between their CSP and GoC networking using SCED infrastructure.			
Video Submission				

MC No.	Requirement Description	Compliant		Reference (Proposal Page No.)
		Yes	No	
MC-56	The Bidder must provide a narrated video (DVD) presentation in MP4 file format. The video presentation must demonstrate the requirements stated in the Mandatory Capabilities that are referenced below. The video presentation should not be longer than one hour and must not be a sales presentation. The Bidder's video submission must support the Bidder's written submission and visibly demonstrates the following mandatory requirements: • MC-04 • MC-05 • MC-07 • MC-08 (a. to e. inclusive) • MC-12			

4.0 Point Rated Criteria

Rated requirements are elements of the functional, technical and management components of the Solution that are assigned numeric values to identify the maximum points that can be scored for each element. Rated requirements are used to determine the relative merit of each proposal and the best overall value to Canada.

Bids will be evaluated and scored on the basis of highest total score. Available points are specified in the table inserted below. Each point rated technical criterion should be addressed separately and should include a reference to the page number in the proposal for the purposes of evaluation.

The following table summarizes the overall point allocation for the following point rated criteria.

Rated Point Allocation Summary

Corporate Experience and Project Management (PRM)	Functional Capabilities (PRF)	Technical Capabilities (PRT)	Total
300	1642	867	2809
11%	58%	31%	100%

4.1 Point Rated Corporate and Management Criteria

PRM No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Corporate Experience				
PRM-1	**Corporate Experience: maximum 50 points** The Bidder should demonstrate: 1. 1 to 5 years of experience in delivering software solutions and executing solution configuration, integration, implementation and support work after contract award. (maximum 5 points)	1 point for each year of experience in delivering software solutions up to a maximum of 5 points		
	2. More than 5 years of experience delivering business solutions and executing solution configuration, integration, implementation and support work after contract award. (maximum 15 points)	3 points for each year of experience above 5 years delivering business and executing solution configuration, integration, implementation and support work up to a maximum of 15 points		
	3. 1 to 5 years of experience delivering software solution, designed to help law enforcement or government agencies through analysis, case management and coordination across multiple jurisdictions. (maximum 5 points)	1 point for every year of experience delivering software solutions designed to help law enforcement or government agency through analysis, case management and coordination across multiple jurisdictions up to a maximum of 5 points		
	4. More than 5 years of experience delivering software solution, designed to help law enforcement or government agencies through analysis, case management and coordination across multiple jurisdictions. (maximum 15 points)	3 points for every year of experience above 5 years delivering software solutions designed to help law enforcement or government agency through analysis, case management and coordination across multiple jurisdictions up to a maximum of 15 points		

PRM No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	5. 1 project or more experience in the delivery of cybercrime related solutions through analysis, intelligence and operational coordination for a five (5) Eye Country (Canada, Australia, New Zealand, the United Kingdom and the United States of America). (Maximum 10 points).	2 points for each relevant project cited up to a maximum of 10 points		
PRM-2	**Solution Delivery Qualifications and Experience: maximum 40 points** 1. (Maximum 10 points): The Bidder should have completed one reference project that included a complete installation and deployment of the Software Solution, where the Bidder provided the following professional services), at a minimum: a) Design; b) Configuration and Implementation; c) Integration and Interfaces; d) Training of Users, system administrators, and technical support staff; and e) Solution Support.	2 points for each of the elements addressed up to a maximum of 10 points		
	2. The Bidder should describe the tasks undertaken to deploy the Solution in this reference project. (maximum of 10 points)	0 points: no information or incomplete description of how the bidder meets the requirement. or the bidder doesn't sufficiently address the requirement 6 points: detailed description provided which sufficiently addresses the requirement. 10 points: a complete in-depth description provided which fully meets and exceeds the requirement.		

PRM No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	3. The Solution in this reference project should currently be in use for the purpose of managing criminal case investigations and analytical output from start to finish. (maximum of 10 points)	0 point if referenced project not in use; 10 points if reference project is still in use.		
	4. The Bidder should have provided the professional services described in the above within the last three years prior to the closing date of this RFP. (maximum 10 points)	0 point if professional services provided is not within the last 3 years 10 points if professional services provided is within the last 3 years		
PRM-3	**Senior Contract Project Manager (CPM) Qualifications. Maximum 50 points** The bidder should demonstrate the number of years beyond the mandatory 10 years that the candidate Senior CPM has served as a Senior Project Manager or a Project Executive or equivalent as of bid closing, managing major IM/IT projects or providing advice to Senior Management. (maximum 50 points)	50 points (5 points for each year beyond the mandatory 5 years - to max. of 10 years)		
Project Management				
PRM-4	**Solution Implementation Schedule. maximum 40 points**			

PRM No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	The Bidder should provide an implementation schedule; 1. Describing the; a. Schedule b. Sequence of Activities c. Dependencies d. Start and End Dates e. Time Estimates (Maximum 25 points)	5 points for each of the elements addressed up to a maximum of 25 points		
	2. Describing the scope of the work including: a. Scope Definition b. Milestones c. Events d. Deliverables (Maximum 10 points)	0 points: no information or incomplete description of how the bidder meets the requirement. or the bidder doesn't sufficiently address the requirement 6 points: detailed description provided which sufficiently addresses the requirement. 10 points: a complete in-depth description provided which fully meets and exceeds the requirement.		
	1. Describing the processes for managing the implementation schedule and supporting lower level schedules throughout all stages of the implementation lifecycle. (maximum 5 points)	0 points: no information or incomplete description of the requirement 3 points: detailed description provided which sufficiently addresses the requirement. 5 points: a complete in-depth description provided which fully meets and exceeds the requirement.		

PRM No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRM-5	**Solution Installation Plan. maximum 40 points** The Bidder should provide a preliminary Solution Installation Plan to demonstrate the following: 1. Understanding of the solution installation requirements (maximum 10 points) 2. How the proposed Solution will be effectively and efficiently implemented for the entire scope of work defined in the SOW, including planning for; a. Configuration b. Integration c. Implementation d. Transition activities e. Solution Support (maximum 10 points) 3. Installation Issue and Risk including; a. Category b. Likelihood c. Impact d. Escalation process e. Mitigation measures (maximum 10 points) 4. Expected contribution of the RCMP Technical Authority to the Solution installation process. (maximum 10 points)	For each sub rated criteria: 0 points: no information or incomplete description of how the bidder meets the requirement. or the bidder doesn't sufficiently address the requirement 6 points: detailed description provided which sufficiently addresses the requirement. 10 points: a complete in-depth description provided which fully meets and exceeds the requirement.		

PRM No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRM-6	**Project Management Plan. maximum 45 points** The Bidder should demonstrate: 1. How it plans to manage the execution of the contract and specifically addressing the measures, processes and mechanism it proposes to undertake to manage and deliver the goods and services under the final contract. (maximum 5 points) 2. The Bidder should provide a contract organization chart that identifies the contract governance structure, the contract team structure, including the executive sponsor, the senior CPM, and the interrelationship with the RCMP team members. Roles and responsibilities of the bidder team members should be defined. (maximum 5 points)	For each rated sub criteria: 0 points: no information or incomplete description of how the bidder meets the requirement. or the bidder doesn't sufficiently address the requirement 3 points: detailed description provided which sufficiently addresses the requirement. 5 points: a complete in-depth description provided which fully meets and exceeds the requirement. 10 points (5 points each)		
	3. The bidder should also demonstrate in its Project Management Plan, how it intends to manage the following components of the management of the project: a. Scope b. Schedule c. Cost d. Quality e. Human Resources f. Communications g. Information Management	Maximum 5 points for each element (a, …, g) for a maximum 35 points		

PRM No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	(maximum 5 points for each element for a maximum 35 points)			
PRM-7	**Change Management. Maximum 10 points** The Bidder should provide a Change Management Plan including; 1. Approach and process that describes how the Bidder will provide a change management process within its methodology (maximum 5 points) 2. Activities and roles to manage and control change during the execution of the contract. (maximum 5 points)	For each rated sub criteria: 0 points: no information or incomplete description of how the bidder meets the requirement or the bidder doesn't sufficiently address the requirement. 3 points: detailed description provided which sufficiently addresses the requirement. 5 points: a complete in-depth description provided which fully meets and exceeds the requirement. 10 points (5 points each)		
PRM-8	**Risk Management. maximum 10 points** The Bidder should describe the areas of risk associated with the project implementation and how it intends to mitigate, manage, and report these risks during project implementation. (maximum 10 points)	0 points: no information or incomplete description of how the bidder meets the requirement. or the bidder doesn't sufficiently address the requirement 6 points: detailed description provided which sufficiently addresses the requirement.		

PRM No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
		10 points: a complete in-depth description provided which fully meets and exceeds the requirement		
PRM-9	**Issue Management. Maximum 15 points** The Bidder should demonstrate how it will manage issues that may be encountered during NCS implementation. The issue management plan should describe: 1. Potential areas of issues associated with the implementation of the project (maximum 5 points) 2. Processes and procedures used to manage and report issues internally and externally with the Project Authority during project implementation (maximum 5 points) 3. Processes and procedures by which issues related to the implementation of the project will be escalated to an identified corporate executive for decision and resolution (maximum 5 points)	For each rated sub criteria: 0 points: no information or incomplete description of how the bidder meets the requirement. or the bidder doesn't sufficiently address the requirement 3 points: detailed description provided which sufficiently addresses the requirement. 5 points: a complete in-depth description provided which fully meets and exceeds the requirement. 15 points (5 points each)		
Corporate Qualifications and Contract Management - Total Score ▶			**xx/300**	

5.0 Point Rated Functional Criteria

Bids will be evaluated and scored as specified in the table inserted below.

Rating	Definition
Demonstrated	Complete, in-depth description of how the bidder has demonstrated the requirement.
Not Demonstrated	Incomplete or limited description of how the bidder has demonstrated the requirement.

The Point-rated Functional Criteria (PRF) describe how effectively a Contractor can meet the project's requirements.

5.1 PUBLIC REPORTING POINT RATED CRITERIA

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Public Reporting				
PRF-1-1	The Bidder should describe how its proposed Solution automatically processes Public Complaint Files that have been captured via the National Cybercrime and Fraud Reporting System (NCFRS).	Demonstrated: 10 points Not Demonstrated: 0 points		
		Public Reporting - Total Score ▶		**xx/10**

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Adaptive Case Management Capabilities				
Create Tickets				
PRF-2-1	**Receive and Parse Submissions** The Bidder should describe how its proposed Solution automatically processes all submissions and service requests received via email, the Police and Partner Portal (P3) or Public Complaint including: a. Receive Submissions and Service Requests from multiple email addresses b. Storing the original email, attachments and all metadata as received c. Creating and storing a Hash value of the email and each attachment d. Maintaining a copy of all original data in read-only format e. Storing data received via P3 Template/Fields, and Parse data including: f. Email body g. Metadata h. Image and Text Attachments including attachment metadata i. Structured, semi structured and un-structured attachments	Maximum 45 points (5 points each)		
PRF-2-2	**Create Ticket** The Bidder should describe how its proposed Solution will automatically create and validate a Ticket based on an email, a P3 Submission or Request or a Public Complaint received via NCFRS including: a. Creating the Ticket with information populated into correct fields, b. Validating mandatory fields, dates, postal codes, province, city, country fields	Maximum 21 points (3 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	c. Linking attachments to the Ticket d. Assigning a unique identifier to the Ticket e. Determine whether the Submission is within NC3 mandate f. Determining the Ticket Type g. Routing the Ticket			
PRF-2-3	**Handle Exploitive Content** The Bidder should describe how its proposed Solution handles exploitive material (for example, material likely to cause offence such as pornographic images of children) including: a. Detecting exploitive content in Submissions b. Routing such submissions for Exception Handling c. Removing exploitive material from a submission, and d. Forwarding a cleansed Submission for completion of processing	Maximum 20 points (5 points each)		
PRF-2-4	**Currency Conversion** The Bidder should describe how its proposed Solution provides a currency conversion utility with the ability to calculate Canadian Dollar (CAD) equivalents including: a. Fiat currency conversion b. Cryptocurrency conversion c. Using current conversion Rate d. Using a historical conversion rate (a date when the cybercrime took place)	Maximum 20 points (5 points each)		
PRF-2-5	**Review Tickets** The Bidder should describe how its proposed Solution allows an NC3 User to review Tickets that have been created by the Solution including: a. confirming population of Ticket fields b. modifying the Ticket to manually parse missed entities	Maximum 20 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	c. removing erroneously parsed entities d. making corrections as necessary			
PRF-2-6	**Manage Tickets** The Bidder should describe how its proposed Solution allows and supports management of Tickets including: a. Automatic Routing Based on Workflow Rules b. Search c. Edit d. Cancel e. Attach notes f. Add attachments g. Merge/Unmerge h. Identify Master Ticket i. Split j. Manually Re-Route (for example; Escalate to Supervisor) k. Print	Maximum 33 points (3 points each)		
	Triage and Assess Submissions			
PRF-2-7	**Internal and External Correlation** The Bidder should describe how its proposed Solution automatically correlates new Submission data to existing data in the NCS Cyber Data Repository, as well as external sources and stores the results including: a. Storing Results b. Ranking and Scoring Results Matching methods including: c. Exact word or phrase match d. Keyword matching	Maximum 34 points (a. and b. 5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	e. Proximity f. Synonym matching g. Fuzzy matching h. Concept matching i. Account for Obfuscation j. Multi-lingual matching	(c. to j. 3 points each)		
PRF-2-8	**Advanced Correlation** The Bidder should describe how its proposed Solution uses Natural Language Processing to support advanced data correlation including: a. Topic and Content Recognition b. Mandate Identification	Maximum 20 points (10 points each)		
PRF-2-9	**Merge Tickets and Files** The Bidder should describe how its proposed Solution supports user confirmed merging of Tickets, Files and Projects based on correlation (in cases when a new Ticket is related to an existing Ticket, File or Project). Merge must be confirmed by a User.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-2-10	**Track and Record Enrichment Activities** The Bidder should describe how its proposed Solution allows an NC3 User to log their ad hoc activities related to File enrichment such as queries to external or open sources.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-2-11	**Set and Manage Severity Scores** The Bidder should describe how its proposed Solution supports automatic Submission Severity Score calculation including:	Maximum 20 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	a. Calculation based on Submission Contents b. Iterative recalculation as necessary, based on results of each enrichment activity c. Using configurable Severity Matrix business rules d. Allowing an NC3 User to override a system calculated Severity Score			
PRF-2-12	**Review Triage Results** The Bidder should describe how its proposed Solution allows an NC3 User to review all results of all Correlation and External System queries.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-2-13	**Identify Submissions of Interest** The Bidder should describe how its proposed Solution supports automatic identification of Submissions that are of interest to sections within the NC3, and triggers the required Notification taking into account: a. Section specific Prioritization Business Rules b. Files that are "in progress" c. Section specific Watchlists	Maximum 15 points (5 points each)		
PRF-2-14	**Manual Routing** The Bidder should describe how its proposed Solution supports File routing including: a. allowing an NC3 User to refer a File to another NC3 Section or User b. allowing an authorized NC3 User to take ownership of a File from another Section	Maximum 10 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	For example, a File being processed by Intake Section may be taken by the Intelligence Section based on a Prioritization Business Rule or Correlation Notification.			
PRF-2-15	**Identify Exceptions** The Bidder should describe how its proposed Solution supports automatic identification of Files that require Exception Handling. Exceptions include non-mandate submissions, insufficient information provided to run business rules, VIP content.	Demonstrated: 10 points Not Demonstrated: 0 points		
	Work Queues			
PRF-2-16	**Manage Work Items** The Bidder should describe how its proposed Solution allows an NC3 User to: a. Access Work Queues b. Drill down on work items to access details and complete task(s) c. Filter work items on attributes d. Search work items e. Sort work items f. View work items with varying levels of detail displayed (for example; File with Task View visible vs File summary view) g. Save Work Queue view preferences h. Assign Work Items i. Self-assign (Pull) work items j. Re-assign a work item to another individual or return a work item to a pool of work items k. Add a note to a work item l. Add a diary date to a work item m. Change the state of a work item (for example; under review, complete or rejected)	Maximum 26 points (2 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRF-2-17	**Mixed Workflows** The Bidder should describe how its proposed Solution supports flexible workflows that allow for: a. Sequential b. Parallel c. Mixed workflows For example, a Submission may be worked on by 3 different NC3 Users/Groups simultaneously.	Maximum 9 (3 points each)		
	Manage Files and Projects			
PRF-2-18	**Manage Files and Projects** The Bidder should describe how its proposed Solution supports all aspects of File and Project Management through a complete life cycle including: a. Searching b. Viewing c. Printing d. Editing information e. Enrichment f. Adding notes or attachments g. Linking and unlinking Tickets to Files, Files to other Files, Files to Projects h. Identify Master File i. Managing Tasks j. Checklists k. Managing Status l. Referral	Maximum 28 points (2 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	m. Limiting access based on RBAC/ABAC Permissions n. Cancelling			
PRF-2-19	**File Referral** The Bidder should describe how its proposed Solution supports referral of Tickets, Files and Projects to external partners.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-2-20	**File History** The Bidder should describe how its Solution provides an NC3 User with a means of managing, accessing and viewing past versions of Ticket, File and Project fields or attachments via the NCS User interface.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-2-21	**Manage Data Preservations** The Bidder should describe how its proposed Solution supports the management of all aspects of Data Preservation Files through their complete life-cycle including; a. Receipt of a Data Preservation Request b. Review and as necessary, manually capture Data Preservation Requests c. Generating Preservation Demand Forms with signature (PDF) d. Managing Status of Preservation Demands e. Issuing Preservation Demands via Email f. Capturing requests to Extend Data Preservations g. Generating Preservation Order Forms h. Issuing Preservation Orders via Email i. Managing Status of Preservation Orders including renewals and j. Recording reference to a Mutual Legal Assistance Treaty (MLAT)	Maximum 40 points (4 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRF-2-22	The Bidder should describe how its proposed Solution is capable of attaching PDFs (for example; data preservation forms, notifications and situation awareness reports) to emails.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-2-23	The Bidder should describe how its proposed Solution is capable of supporting review and approval of reports, notifications or other outputs (by authorized NC3 Users) prior to distribution.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-2-24	**Disclosure Package** The Bidder should describe how its proposed Solution allows an NC3 User to create a configurable, printable "Disclosure Package" containing selected or all contents and activities related to a Ticket, File or Project including: e. related data f. metadata g. activity log contents h. system audit logs and i. attachments	Maximum 10 points (2 points each)		
PRF-2-25	**Output to File and Print** The Bidder should describe how its proposed Solution, for all Tickets, Files and Projects, supports the following packaging and printing functionality: a. Allow an NC3 User to print any or all contents to printer or electronic copy (for example; .pdf, .xls or .doc)	Maximum 15 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	b. Automatically apply configurable information security designation and TLP sharing watermarks to all outputs based on the printed data c. Allow an NC3 User to apply configurable watermarks on all outputs			
PRF-2-26	**Create and Manage Projects** The Bidder should describe how its Solution will provide an NC3 User with the ability to create and manage Project's including: a. Assigning Unique Project Number b. Linking File(s) to the Project c. Capturing Project Details (for example; Project Name (unique), Synopsis, Priority, Start Date and End Date) d. Assigning Security Designation (for example; Protected B) e. Assigning NC3 and P3 Users to the Project f. Managing permissions and assigned Users g. Manage Implicated Parties h. Manage Project Status i. Manage Tasking	Maximum 27 points (3 points each)		
Adaptive Case Management Capabilities - Total Score ▶			**xx/493**	

5.2 POLICE AND PARTNER PORTAL (P3) CAPABILITIES POINT RATED CRITERIA

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Police and Partner Portal (P3) Capabilities				
Query NCS				
PRF-3-1	**Query NCS Cyber Data Repository** The Bidder should describe how its proposed Solution provides a P3 User with the ability to query the NCS Cyber Data Repository including: 1. Search Functionality a. Searching methods (Exact, fuzzy, proximity, wildcard, synonym, date ranges, cross-lingual) b. Silent Query Indicator c. Capture Search Reason d. Save a Search / Recall a Search e. Search Scoring/Ranking f. Ensure mandatory criteria is entered g. Auto-Complete search criteria 2. Search Criteria: a. Metadata b. Reference Numbers c. Data Originator d. Indicators of Compromise e. Unstructured Text, Topics f. File Types (for example; Service Request, Public Complaint Report or Data Preservation) g. Cybercrime Location h. Date(s) (for example; Ticket/File/Project Date or Date Information Added) i. Target Specific Data (for example; Watchlist(s), Query History, email body or Full Repository)	Maximum 32 points (1a. to 1g. 2 points each) (2a. to 2i. 2 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRF-3-2	**Display Search Results** The Bidder should describe how its proposed Solution displays relevant search results to the P3 User. By default, results should be sorted by relevance to the query. The Search Results should allow the user to: a. Filter b. Sort c. Print d. View Highlighted search terms in the result	Maximum 12 points (3 points each)		
Submit Service Request				
PRF-3-3	**Create Service Request** The Bidder should describe how its proposed Solution provides a P3 User with the ability to create various types of Service Requests using data input templates to facilitate capture and validation of relevant information based on request type. Service Requests can be submitted to NC3 as well as other authorized P3 Agencies.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-3-4	**View Acknowledgements and Results** The Bidder should describe how its proposed Solution provides a P3 user with the ability to view: a. Service Request acknowledgements b. Service Request results	Maximum 20 points (10 points each)		
Submit Cybercrime Information				
PRF-3-5	**Cybercrime Information Submission**	Maximum 10 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	The Bidder should describe how its proposed Solution supports the submission of structured or unstructured Cybercrime information to the NC3 using the P3 including the capability to indicate the following: a. Information Context b. Instructions to NC3 c. Data Sharing Classification d. Data Security Designation and e. Reference to previous Submissions.	(2 points each)		
PRF-3-6	**Capture and Submit Public Complaint File** The Bidder should describe how its proposed Solution allows a P3 User to capture a Public Cybercrime Complaint File, using a Public complaint data capture user interface, and submit it to the NC3 for processing.	Demonstrated: 10 points Not Demonstrated: 0 points		
Receive Notifications, Messages and Requests				
PRF-3-7	**P3 Watch List** The Bidder should describe how its proposed Solution supports P3 Agency Notification based on correlations to records in the Agency's P3 Watchlist.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-3-8	**Manage Messages and Requests** The Bidder should describe how its proposed Solution allows the P3 User to: a. Monitor Messages and Requests received from the NC3 or other P3 Agencies b. Maintain the status of Messages and Requests (for example; Read, Un-read, In-Progress, Responded or Closed)	Maximum 30 points (10 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	c. Create a structured response to the applicable NC3 request			
PRF-3-9	**P3 Update File** The Bidder should describe how its proposed Solution will allow a P3 User to perform the following actions related to a Ticket, File or Project to which the P3 User has access: a. make a status update b. add notes c. add attachments d. edit and add data in fields.	Maximum 12 points (3 points each)		
Access Files				
PRF-3-10	**Access Public Reports** The Bidder should describe how its proposed Solution provides the P3 User with access to the Public Complaint Reports that are made available to their Police of Jurisdiction including providing: a. Searchable, filterable access b. Indication of severity, scoring, and added enrichment Public Complaint Files will vary widely in terms of actionable information. Some may include NC3 developed enrichment, some may not include enough information to warrant further investigation. Minimally, the Solution should allow the P3 User to differentiate between these Files.	Maximum 20 points (10 points each)		
PRF-3-11	**File and Project Referrals** The Bidder should describe how its proposed Solution provides a P3 User with access to Files and Projects, including all releasable	Demonstrated: 10 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	enrichment and actionable intelligence; that are referred to the P3 Partner by the NC3.	Not Demonstrated: 0 points		
PRF-3-12	**Manage File Status** The Bidder should describe how its proposed Solution allows the P3 user to manage the status of Files on their queue to indicate whether the File is being, or has been, actioned and what action is or has been taken. This status management capability is intended to provide the NC3 with information on referrals that are being processed by P3 Partners.	Demonstrated: 10 points Not Demonstrated: 0 points		
Register Data Preservation				
PRF-3-13	**Register Data Preservation** The Bidder should describe how its proposed Solution supports capture of Data Preservation information for the purposes of deconfliction including: a. Subject of the data preservation b. Data to be preserved c. Data Holder information d. Foreign or Domestic Indicator e. Preservation Demand or Order Indicator (Domestic only) f. Criminal Code Statute supporting the Data Preservation g. Applicable dates (Start, End, Extended) h. Local case # and contact information i. Production Order/MLAT Indicator	Maximum 18 points (2 points each)		
PRF-3-14	**Manage Registered Data Preservations** The Bidder should describe how its proposed Solution allows a P3 User to manage its registered Data Preservations including; a. Cancel the Preservation,	Maximum 15 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	b. Adjust the dates and update details of a Registered Data Preservation c. Indicate that the Data Preservation has led to a Production Order			
Access Knowledgebase / Directory				
PRF-3-15	**Knowledgebase** The Bidder should describe how its proposed Solution will support a P3 Users access to a knowledgebase including; a. Browse b. Search c. View d. Download e. Print The Knowledgebase is expected to contain content such as, Educational resource content and links, Job aids and Templates, Frontline officer intake checklists, Scenario guidelines and tips and Precedents and case law.	Maximum 10 points (2 points each)		
PRF-3-16	**Directory of Contacts** The Bidder should describe how its proposed Solution provides P3 users with a searchable Directory of contacts including organizations such as Internet Service Provider contacts, cryptocurrency exchanges, IT Security contacts, LE cybercrime subject experts, cybercrime and fraud investigator contacts. Search parameters should include criteria such as expertise, contact name and location.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-3-17	**Catalogue of Tools, Services and Sandbox**	Maximum 12 points (4 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	The Bidder should describe how its proposed Solution allows a P3 user to browse, search, find and schedule usage of software tools available via the NC3 cybercrime "toolbox/sandbox" including: a. Searching by tool type/features b. Access to tool availability status and schedule and c. Schedule time to use a tool.			
Request Malware Cross-Reference				
PRF-3-18	**Capture Malware Cross-reference Request** The Bidder should describe how its proposed Solution provides a P3 User with the ability to Capture and submit a Malware Cross-Reference Request including: a. Local Case Number b. Synopsis / Context c. Malware Sample to Submit indicator (submitted separately) d. Related Indicators of Compromise e. Submitted for Intelligence Only f. Related to ongoing investigation g. Findings to be used in Judicial Discovery.	Maximum 14 points (2 points each)		
PRF-3-19	**Submit Malware Sample** The Bidder should describe how its proposed Solution provides a P3 User with the ability to submit their malware sample without endangering the NC3 system environment. The solution should securely segregate Malware samples from all RCMP data and systems.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-3-20	**Review Malware Analysis Result**	Demonstrated: 10 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	The Bidder should describe how its proposed Solution allows a P3 User to be notified of, and then access, the results of the Malware Cross-Reference Analysis.	Not Demonstrated: 0 points		
Manage Preferences				
PRF-3-21	**Manage P3 Agency Profile** The Bidder should describe how its proposed Solution allows an authorized P3 user to set configuration parameters that are specific to their P3 Agency including: a. Local email address for notifications b. Notification Email Options (for example Hourly, Daily or Weekly) c. Contact Information d. Capability Profile **e.** Related Agency(s) – Superior/Subordinate	Maximum 10 points (2 points each)		
PRF-3-22	**Manage P3 Watch List** The Bidder should describe how its proposed Solution allows a P3 user to manage a Watch List (for example; list of Indicators of Compromise, Tools Techniques and Procedures (TTP), Topics and BOLO) of specific interest to that user's organization. Correlation to a P3 Watch List entry will, depending on the entry's notification rules, result in a notification to the P3 Agency.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRF-3-23	**Manage Public Report Viewing Criteria** The Bidder should describe how its proposed Solution allows a P3 user to maintain its Public Report notification and viewing parameters. These parameters will allow the P3 Agency to tailor their notifications and Public Report work queues to show reports that meet or surpass thresholds or "Take on Criteria" for the agency.	Demonstrated: 10 points Not Demonstrated: 0 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	Police and Partner Portal (P3) Capabilities - Total Score ▶		xx/315	

5.3 FUNCTIONAL CAPABILITIES POINT RATED CRITERIA

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Functional Capabilities				
Notifications				
PRF-4-1	**Auto Notification** The Bidder should describe how its proposed Solution automatically supports notifications to implicated users, groups, LE Agencies or Cybercrime Partners including; a. Configurable Triggers b. Accounting for data sharing, Role Based Access Control and Attribute Based Access Control Triggers should include Discovery of correlations – Watchlist, Query, New Data Added, File modifications and Referrals.	Maximum 20 points (10 points each)		
PRF-4-2	**Manual Notification** The Bidder should describe how its proposed Solution allows an NC3 User to manually send a Notification to a: a. User b. Group c. LE Agency d. Cybercrime Partner The contents of manual notifications will also be subject to disclosure limitations.	Maximum 12 points (3 points each)		
PRF-4-3	**Email and Text Notification** The Bidder should describe how its proposed Solution supports configurable Notifications to NC3 Users, cybercrime partners and LE agencies by;	Maximum 20 points (10 points for email capability)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	a. Email b. Text message In the event that a high-priority Notification is sent during off-hours (automatically or manually) the Solution should be capable of using email and Text messaging to ensure real-time delivery of the Notification. Notifications will either be self-contained or instruct the recipient to access the P3 or NC3 for further details.	(10 points for Text message capability)		
PRF-4-4	**Non-Deliverable / Restricted Notifications** The Bidder should describe how its proposed Solution notifies an NC3 User if a notification cannot be delivered due to a data sharing restriction or Role Based Access Control or Attribute Based Access Control rule.	Demonstrated: 10 points Not Demonstrated: 0 points		
Dashboards				
PRF-4-5	**Dashboard Content and Drill-Down** The Bidder should describe how its proposed Solution supports configurable NC3 and P3 Dashboards including: a. NC3, P3 and User Role Specific Content b. Access to Summary level information of Notifications, Messages, Requests and Referrals c. Ability to Drill down to details, Messages, Requests, Referrals d. Search, Filter and Sort Notifications e. Local Jurisdiction Statistics f. Regional and National Statistics g. Trends (for example; Victimization and Threat related, campaign, thematic and temporal)	Maximum 36 points (3 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	h. Fraud/Cyber Statistics and trends: regional local, national level with thematic mapping i. Volumes: Queries, correlations discovered j. Work in Progress: Intake, Assessment, Intelligence Files, Operational Coordination Files, Projects including status k. Tiles displaying graphical views of aggregated data **l.** Geospatial representations and Heatmaps			
PRF-4-6	**Dashboard Customization** The Bidder should describe how its proposed Solution allows an NC3 User to customize their dashboard view by selecting from predefined contents/tiles.	Demonstrated: 10 points Not Demonstrated:0 points		
Data Analytics				
PRF-4-7	**Analyzing Data** The Bidder should describe how its proposed Solution allows the user to work in an interactive and collaborative data science environment to manipulate data, code and models associated with various data sources, Files and Projects including; a. Temporarily storing data (to build timelines and test hypothesis) b. Cleansing and transforming data c. Building analytical models, write code, execute code, in whole or in part d. Applying version control to analytics projects e. Associating or sharing projects and contained data / models with other users and Files f. Discovery of Correlations and Linkages and triggering associated notifications if required	Maximum 40 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	g. Visualizing data (for example; raw data, cleansed data, results of code execution and results of models) h. Export or associating models, outputs and analytics projects for sharing with external users			
PRF-4-8	**Data Visualization** The Bidder should describe how its proposed Solution provides the means to produce and display charts and diagrams including; a. Link charts b. Flow charts c. Event and Time Series charts d. Geospatial maps, heat maps, choropleth, dot density e. Other graphical depictions from the data enriched by the analytic tool.	Maximum 25 points (5 points each)		
PRF-4-9	**Save View and Print Analytics Results** The Bidder should describe how its proposed Solution supports comprehensive Intelligence Reports containing graphical representations of the data and images including: a. Saving b. Viewing c. Printing d. exporting (exportable file format such as Adobe Acrobat PDF)	Maximum 20 points (5 points each)		
PRF-4-10	**Review and Share Analytics Reports** The Bidder should describe how its proposed Solution allows a User to review and share Analytics Reports, outputs or related information (Status, Analysis Results; Partial or Final) with selected agencies/users.	Demonstrated: 10 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
		Not Demonstrated:0 points		
PRF-4-11	**Redaction** The Bidder should describe how its proposed Solution allows a user to selectively redact information in outputs to protect sources or other individually identifiable persons that are not subjects of a File, while retaining an original un-redacted version.	Demonstrated: 10 points Not Demonstrated:0 points		
Configuration and Administration				
PRF-4-12	**Dashboard Tiles** The Bidder should describe how its proposed Solution provides an authorized NC3 User with the ability to create, modify and delete Dashboard Tiles that can be pinned to custom dashboards. Dashboard Tiles should include permissions to tailor content to various user levels.	Demonstrated: 10 points Not Demonstrated:0 points		
PRF-4-13	**Manage Code Tables** The Bidder should describe how its proposed Solution provides authorized NC3 User (Administrator) with the ability to manage (add, modify, delete) code table contents used for purposes such as validating encoded data inputs and displaying pick lists in the user interface.	Demonstrated: 10 points Not Demonstrated:0 points		
PRF-4-14	**Manage On-Line Help Content** The Bidder should describe how its proposed Solution provides an authorized NC3 User with the ability to manage on-line help content.	Demonstrated: 10 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
		Not Demonstrated:0 points		
PRF-4-15	**Manage Partner and Client Directory** The Bidder should describe how its proposed Solution provides an authorized NC3 User with the ability to manage profile information related to Cybercrime Partners, Law Enforcement Agencies and all other stakeholders with which the NC3 interacts. Profiles include information such as: a. Partner / Client Type b. Location c. Contact Information d. Level of Cybercrime Expertise e. Escalation Contact and Procedure f. Law Enforcement Agency Referral Preferences g. Thresholds	Maximum 14 points (2 points each)		
PRF-4-16	**Manage Directory of Contacts** The Bidder should describe how its proposed Solution provides an authorized NC3 User with the ability to manage Cybercrime related resource Contact and Subject Matter expert information that will be made available to Police and Partners via the P3 including: a. Create b. Modify c. Delete d. Search e. Sort and Filter.	Maximum 10 points (2 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRF-4-17	**Manage Templates and Rules** The Bidder should describe how its proposed Solution supports management of Templates and rules including: a. Notification Template management and editing; including content and permissions b. Configure P3 Response Templates c. Configure P3 Submission Templates d. Rules to set Notification modes; indicate when email, SMS text message or P3 Notification are required (or any combination).	Maximum 20 points (5 points each)		
PRF-4-18	**Create and Manage Workflows** The Bidder should describe how its proposed Solution provides authorized NC3 Users with the ability to manage workflows including: a. Create Workflows b. Define and Manage Routing c. Define and Manage Tasks d. Define related User groups	Maximum 20 points (5 points each)		
NCS Repository Query				
PRF-4-19	**NCS Query** The Bidder should describe how its proposed Solution provides the ability to query on applicable field or attribute in the NCS Data Repository. The Solution should by default, if more than one criterion is used, return results that match all criteria (per chosen search method).	Demonstrated: 10 points Not Demonstrated:0 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRF-4-20	**Advanced Search Techniques** The Bidder should describe how its proposed Solution supports searching methods including: a. Exact word, phrase or Topic matching b. Proximity searches c. Proximity searches within sentences or paragraphs d. Wildcard searches e. Boolean search f. Synonyms of words specified search criteria g. Fuzzy Searching (for example; Soundex) h. Obfuscated words (for example; disco = d1$c0, mysite.com = mysite dot com) i. Cross-Language searching j. Keyword searching k. Concept Searching l. Consideration for Non-native text and multi-lingual searching m. Any combination of search criteria identified above within the same query	Maximum 26 points (2 point each)		
PRF-4-21	**Search Result Ranking** The Bidder should describe how its proposed Solution generates, and returns to the user, a query list of results individually ranked on a grade of similarity with the query criteria.	Demonstrated: 10 points Not Demonstrated:0 points		
PRF-4-22	**Search Result Content** The Bidder should describe how its proposed Solution provides relevant search results including: a. Result Ranking (Score)	Maximum 30 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	b. Default Sorting Order (for example; Score, Applicable Date or Alphabetic (if applicable)) c. Match Type (Exact, Proximity) d. Data Matched To (for example; Query History, Data Preservation, Data Submission or Complaint File) e. Result Date information (for example; Date Data added or Date last updated) f. Contact Information			
PRF-4-23	**Result Viewing Features** The Bidder should describe how its proposed Solution provides users with the ability to: a. Filter on results b. Sort results c. Drill-Down/up/through to view related details (for example; Ticket or File)	Maximum 15 points (5 points each)		
PRF-4-24	**Natural Language Query Interface** The Bidder should describe how its proposed Solution provides Users with a natural language query interface including; a. Command line (type in query) b. Form/Template (fill in fields) c. Graphical assisted (drag and drop or select geographical area)	Maximum 15 points (5 points each)		
PRF-4-25	**Save a Search** The Bidder should describe how its proposed Solution provides a user with the option of saving the search criteria for future execution including the ability to:	Maximum 15 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	a. Name a search b. Access to a Search History by name, date, criteria and c. Share a search with other users.			
PRF-4-26	**Silent Query** The Bidder should describe how its proposed Solution supports Silent Query. The Solution should support the following Silent Query Rules: a. Return results of a Silent Query to the querying agency only b. No notification to any other implicated agency with the exception of the NC3 Unit should be triggered c. "Same Query Criteria" notifications are also suppressed by the Silent Query indicator d. Silent Queries will not override notifications to designated NCS internal users. It will apply to notifications to external LE agencies and partners only.	Maximum 20 points (5 points each)		
PRF-4-27	**Silent Hit** The Bidder should describe how its proposed Solution supports a "silent hit" feature (see Glossary of Terms) where, based on tagging of a data entity such as a Watchlist entry, an occurrence is not included in a search result, but the contributor of the data is notified.	Demonstrated: 10 points Not Demonstrated:0 points		
PRF-4-28	**Search Query History** The Bidder should describe how its proposed Solution searches a Query History for similar searches and provides a response to indicate: a. similar criteria b. query reason c. query date **d.** querying agency and user	Maximum 12 points (3 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRF-4-29	**Federated Search** The Bidder should describe how its proposed Solution allows a user to conduct a federated search across all NCS data stores (for example; Data Catalog, Object Stores and Relational Databases) with a single query.	Demonstrated: 10 points Not Demonstrated:0 points		
PRF-4-30	**Handling Query Result Restrictions** The Bidder should describe how its proposed Solution supports query results when RBAC or ABAC restrictions prohibit release of information including: a. Ability to indicate that information exists, and provide contact information, while not releasing the actual details of the information. b. Ability to return no result at all (depending on data sharing rules) c. Ability to notify the NC3 if no result can be released.	Maximum 12 points (4 points each)		
PRF-4-31	**Print and Save Search Result** The Bidder should describe how its proposed Solution provides a user with the ability to manage search results including: a. Printing b. Saving	Maximum 10 points (5 points each)		
Maintain Business Rules and Watch Lists				
PRF-4-32	**Manage Severity Matrix** The Bidder should describe how its proposed Solution supports the creation and management of configurable Severity Matrix Business rules that the Solution will use to derive Severity Scores for Submissions and Service Requests including: a. Service Request Type	Maximum 15 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	b. Applicable Severity Criteria and Rules c. Scores The Solution should support creation of new rules and maintenance of existing rules that are specific to many types of Submissions and Service Requests including: Service Requests from Law Enforcement, Submissions from Law Enforcement and Public Complaint Files from the National Cybercrime and Fraud Reporting System.			
PRF-4-33	**Manage Prioritization Business Rules** The Bidder should describe how its proposed Solution will support the creation and management of Prioritization Business Rules – used to highlight Submissions that are of potential interest to specific sections within the NC3 including: a. Section specific rules b. Section specific watchlists c. Section Specific "of interest" criteria d. Ability to configure rules in near real-time For example, the Intelligence Section might be interested in any submission that concerns ransomware where a municipality in Ontario is victimized. Prioritization Business Rules can be created to flag submissions that meet this criterion to the Intelligence Section.	Maximum 20 points (5 points each)		
PRF-4-34	**Manage Watch Lists** The Bidder should describe how its proposed Solution will allow an NC3 user to create and manage Watch Lists for various sections within the NC3. Watch Lists should support: a. specific Indicators of Compromise such as Monikers or URL b. more complex data such as Tactics Techniques and Procedures	Maximum 10 points (5 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRF-4-35	**Configure Workflow Logic Business Rules** The Bidder should describe how its proposed Solution allows an NC3 User to manage Business Rules related to Workflows including: a. Ability to create and modify rules that dictate workflows b. Ability to indicate rule effective date/times (start and end) c. Ability to support rule modifications without system downtime	Maximum 15 points (5 points each)		
Cyber Toolbox / Sandbox / Knowledgebase Service				
PRF-4-36	**Manage Toolbox Requests and Usage** The Bidder should describe how its proposed Solution supports Partner requests to use cybercrime forensic applications and services provided by the NC3 including: a. Granting access to tools b. Monitoring activities related to tool set-up c. Monitoring tool usage	Maximum 9 points (3 points each)		
PRF-4-37	**Use Results of Forensic Analysis Tools** The Bidder should describe how its proposed Solution is capable of incorporating the results of forensic analysis tools into the NCS Repository for the purposes of correlation, deconfliction and situational awareness including how the Solution will notify NC3 users when correlations are made based on results of tool usage.	Demonstrated: 10 points Not Demonstrated:0 points		
PRF-4-38	**Manage Knowledgebase**	Demonstrated: 10 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	The Bidder should describe how its proposed Solution supports management of Knowledgebase content made available to P3 Users including how content can be provided by P3 Partners, reviewed and edited by the NC3 and published to the Knowledgebase.	Not Demonstrated:0 points		
PRF-4-39	**Manage Catalogue of Services** The Bidder should describe how its proposed Solution allows an NC3 User to manage a catalogue of NC3 services that is made available via the P3 including: a. Create and Modify entries including service descriptions, applicable pre-requisites, usage notes and search criteria b. Manage service availability dates (start and end) c. Delete Entries	Maximum 15 points (5 points each)		
Artificial Intelligence / Machine Learning				
PRF-4-40	**Machine Learning Models** The Bidder should describe how its Solution will deploy machine learning models and Natural Language Processing to bring efficiencies to NC3 processes including; a. Triage and Assessment b. Data Analytics c. Workflow	Maximum 30 points (10 points each)		
PRF-4-41	**Artificial Intelligence (AI) Compliance Standards** The Bidder should describe how its proposed Solution will support the RCMP in complying with Government of Canada's Guiding Principles on	Demonstrated: 10 points		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	use of Artificial Intelligence and the Directive on Automated Decision-Making.	Not Demonstrated:0 points		
PRF-4-42	**Explainable Artificial Intelligence** The Bidder should describe how its proposed Solution ensures that decisions made using Artificial Intelligence are explainable. Explainable methods are required (as opposed to "Black Box" AI) in the event that decisions are questioned during legal proceedings.	Demonstrated: 10 points Not Demonstrated:0 points		
PRF-4-43	**Applications of Machine Learning** The Bidder should describe how its proposed Solution would apply machine learning models to support business needs including: a. Identification of precursors - where events, when seen, may indicate an activity of interest will follow b. Develop victim profiles - where different demographics may require variations in law enforcement support and response levels c. Develop threat actor profiles - with the aim of identifying a threat individual d. Identify enablers and criminal infrastructure - including service providers, dark web markets for software and services, brokers e. Develop profiles for devices, services, locations, "non-human" cyber actors f. Enable simulations - including hypothesis testing (what happens if…?) g. Characterize events - has something been seen before, but looks different now h. Enable intelligence activities - including development of activity flows, commodity flows, crime pattern analysis, financial analysis, market profiles i. Query Optimization	Maximum 39 points (3 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	j. Automated Input Optimization and Response (Contextual advice) k. Sematic Analysis l. Classifying the type of service request or submission based on contents **m.** Recognizing sentiment (self-harm, violence, threats)			
PRF-4-44	**Management of Machine Learning Models** The Bidder should describe how its proposed Solution allows machine learning models to be: a. easily coded b. trained c. tested d. optimized (for example; hyperparameter optimization) e. deployed to production **f.** monitored and maintained	Maximum 18 points (3 points each)		
PRF-4-45	**Monitoring of Machine Learning Models** The Bidder should describe how its proposed Solution allows machine learning models to be: a. Saved, versioned, and retrieved from within the Data Science Environment b. Tracked through performance metrics/measurements once deployed into production	Maximum 10 points (5 points each)		
Natural Language Processing				
PRF-4-46	**Applications of Natural Language Processing** The Bidder should describe how its proposed Solution will use Natural Language Processing named entity data extraction capabilities and Data Analytics to identify valuable data in unstructured data (text and images) including: a. Cybercrime observables and indicators of compromise	Maximum 27 points (3 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	b. Incidents c. Targets d. Adversary and defensive tactics, techniques and procedures (TTPs) e. Campaigns f. Courses of action g. Cyber actors h. Sentiment Analysis i. Multiple Language Capabilities			
Business Intelligence				
PRF-4-47	**Business Intelligence Reporting** The Bidder should describe how its proposed Solution will support real-time, standard, customized and ad hoc reporting related to: 1. Operational Measures a. Number of queries via the Police and Partner Portal b. Number of Malware Cross-Reference requests c. Submissions received d. Assistance requests received/Sent e. Queries processed f. Correlations found g. Intel Files in progress/completed h. Operational Coordination Files in progress/completed i. Number of referrals made/closed j. Partnerships established k. Private partner engagements 2. Strategic Measures a. Cybercrimes and Frauds by type, value, victim, location and other attributes	Maximum 26 points (2 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	b. Trends; Month over Month, Year over Year			
PRF-4-48	**Export to Statistics Canada and Partners** The Bidder should describe how its proposed Solution will support automatic standard, as well as flexible, report and data exports to Statistics Canada - Canadian Centre for Justice Statistics (CCJS) and other external partners.	Demonstrated: 10 points Not Demonstrated: 0 points		
Cross-Reference Malware				
PRF-4-49	**Manage Malware Cross-Reference Requests** The Bidder should describe how its proposed Solution will support the management of Malware Cross-Reference Requests from P3 Partners including: 1. Receipt of Malware Cross-Reference Requests a. Intake Workflow and Case Management b. Correlation to NC3 Malware Libraries (via Hash value comparison) c. Automatic and if necessary manual correlation of Indicators of Compromise provided with the request d. Return of local results or request to submit sample via P3 2. Processing of Malware Samples a. Quarantine Malware Sample b. Create Hash value and store in NC3 Malware Library c. Forward a sample to external Malware Analysis Services for Analysis – retaining quarantined copy d. Manage Outstanding requests e. Receive, store, review and return results of Malware Analysis Services f. Create a Malware Analysis Report or Bulletin for posting to the Knowledgebase	Maximum 20 points (1.a. to 1.d. 2 points each) (2.a. to 2.f. 2 points each)		

PRF No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Automated Enrichment				
PRF-4-50	**Entity Resolution** The Bidder should describe how its proposed Solution will support entity resolution and the identification of links between entities including the following a. De-conflicting and combining on-line or Internet Identities based on common attributes b. Automated entity resolution of Indicators of Compromise c. Manual review of resolved entities d. Ability to separate entities that were erroneously resolved e. Automatically trigger notifications based on resolutions f. View and manipulate entities with a link/network visualization tool	Maximum 18 points (3 points each)		
		Functional Capabilities - Total Score ▶	**xx/824**	

5.4 POINT RATED TECHNICAL CAPABILITY CRITERIA

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Technical Capabilities				
Submission Quarantine				
PRT-5-1	The Bidder should describe how its proposed Solution will ensure the security of the NC3 but also provide maximum threat intelligence to the business by: a. Screening all Submissions, including encrypted content, for malicious content b. Halting processing if malicious content is found c. Ingesting Submission found to be clean **d.** Making the results of screening available for review	Maximum 20 points (5 points each)		
PRT-5-2	The Bidder should describe how its proposed Solution will process exploitive content including: a. Automated Scanning for exploitive content b. Quarantine and exception processing of exploitive content c. Forwarding the submission to the National Child Exploitation Coordination Centre (NCECC) when the submission contains detected child exploitive content d. If the solution has not automatically recognized exploitive content, allow an NC3 user to forward the exploitive content to the NCECC	Maximum 20 points (5 points each)		
PRT-5-3	The Bidder should describe how its proposed Solution will provide a user with a means of reviewing Submissions that have been identified as containing malicious or exploitive content, allow removal of malicious or exploitive content or attachments, and ingest the modified submission.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-4	The Bidder should describe how its Solution supports the secure exchange of information including emails and attachments, using:	Maximum 10 points		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	a. The x.509 standard b. An open source standard for example, Pretty Good Privacy (PGP).	(5 points each)		
Data Import/Export Tools				
PRT-5-5	The Bidder should describe how its proposed Solution will support the import and export of data using common file formats including: a. Import data from another system in XML, and JSON formats b. Export data to another system in XML, and JSON formats c. Import and Export data to an Analysis Tool d. Import and Export data from Open Source Feeds (for example MISP). e. The creation of usable record constructs such as Tickets and Files f. Import and Export structured data files including unstructured data attachments between P3 Partners and the NC3.	Maximum 30 points (5 points each)		
PRT-5-6	The Bidder should describe how its proposed Solution will support the secure exchange of files larger than 1 terabyte including: a. Secure Transfer of Large Files (e.g. greater than 1 Terabyte) b. Seamless integration with the NCS User Interface	Maximum 20 points (10 points each)		
PRT-5-7	The Bidder should describe how its proposed Solution supports compressing and decompressing data using: a. ZIP b. LZH c. 7Zip d. GZIP e. WinRAR	Maximum 10 points (2 points each)		
Data Exchange Standards				

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRT-5-8	The Bidder should describe how its proposed Solution will support the exchange of data to and from external systems using each of the following data exchange standards: a. Structured Threat Information eXpression (STIX) b. Vocabulary for Event Recording and Incident Sharing (VERIS) c. National Information Exchange Model (NIEM) d. Trusted Advance eXchange of Indicators Information (TAXII) e. Law Enforcement Information Data Standard (LEIDS). f. User definable data exchange standards that can be used for importing and exporting data into and out of the Solution	Maximum 12 points (2 points each)		
Information Management				
PRT-5-9	The Bidder should describe how its proposed Solution will support the following information management capabilities: a. Validate that received data is tagged with data sharing and handling security level categorizations b. Enable an NC3 user to manage data categorization codes and manage metadata for NC3 data assets (for example; Data Cataloging). c. Enable a user to indicate that the file contains a subject under the age of 18 d. Ability to assign Handling Codes and Security Level categorizations to data e. Raising an alert for exception processing if the security designation of any information exceeds the system designation of Protected B f. Re-labelling, exporting and purging information that has exceeded security level of Protected B	Maximum 18 points (3 points each)		
PRT-5-10	The Bidder should describe how its proposed Solution provides a user with the ability to manage the physical deletion of data as follows:	Maximum 10 points		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	a. Delete inappropriate or unauthorized data from the system b. Export data into a file prior to its physical deletion	(5 points each)		
PRT-5-11	The Bidder should describe how its proposed Solution supports the ability to reduce data management storage costs by: a. Moving inactive, archived, or Archived data into lower cost storage (for example; Hot vs Cool vs Archive Data Storage) b. Retrieving data from Archive or Cool storage into active (Hot or Cool Storage) c. Providing user configurable time period parameters to automatically set hot, cool and archive retention periods for different data types	Maximum 15 points (5 points each)		
PRT-5-12	The Bidder should describe how its proposed Solution supports archive and purge (logical deletion), including: a. Purging information and data at the end of definable retention period b. Identifying information and data meeting archival criteria c. Providing a data purge confirmation process to allow a user to approve the purge of data and edit the disposition date as necessary d. Accounting for linkages when identifying data to purge. If a linkage exists, the linked data is subject to the retention date furthest in the future e. User configurable time period parameters to automatically set archive and purge retention periods for different record types f. Data purge confirmation functionality in order to expunge or remove data	Maximum 18 points (3 points each)		
PRT-5-13	The Bidder should describe how its proposed Solution can be configured to incorporate external data sources (for example; the	Maximum 15 points (5 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	Enterprise Data Warehouse, or a Legacy DBMS) into a Federated NCS Repository Query capability, including: a. Configuring and managing connections to external data stores b. Dynamically indexing an external data store c. Incorporating the Index into a Federated NCS Repository Query			
Role Based and Attribute Based Access Control				
PRT-5-14	The Bidder should describe how its proposed Solution supports configurable Role Based Access Control and Attribute Based Access Control to functionality and information based on definable user roles and groups. The Bidder should describe how its proposed Solution supports Role Based Access Control and Attribute Based Access Control to limit access based on: a. User / Group Role b. User Location c. Data Sensitivity d. Data Sharing Categorization e. Functionality (View, Query, Add, Update, Delete) f. Data Type (Query Results, Notifications, Files, Projects)	Maximum 18 points (3 points each)		
PRT-5-15	The Bidder should describe how its Solution controls the disclosure of information using Information Sharing codes (for example; Traffic Light Protocol) and Data Security Designations for: a. Notifications b. Messages c. Query Results	Maximum 15 points (5 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Enterprise Integration				
PRT-5-16	The Bidder should describe how its proposed Solution supports the use of Open Standards to provide configurable interfaces (for example; JSON, Restful APIs and asynchronous messaging brokering) for system integration with the following Tools and Components: a. Data Analytics tools b. NLP tools c. Text Extraction tools d. Geospatial tools (Esri) e. Data Visualization tools f. Data Compliance tools g. Public Domain Cybercrime Repositories h. Entity Resolution tools i. Speech-to-Text and Translation tools j. OCR tools k. Network Analysis tools l. Case Management tools m. Statistical Modeling tools n. Business Intelligence / Reporting tools o. Federated Search tools p. Enterprise Warehouse tools	Maximum 32 points (2 points each)		
PRT-5-17	The Bidder should describe how its proposed Solution can be configured to exchange data with external systems using documented interfaces implemented with industry open standard APIs that: a. Use industry open standard bindings and protocols (including but not limited to: REST/JSON or SOAP/XML) b. Expose data as non-proprietary business entity or object schemas	Maximum 15 points (3 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	c. Adhere to the Government of Canada Standards on APIs as defined by: https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html d. Utilize a Service Bus or Event Handler to manage data interactions between systems e. Support OpenAPI or Swagger, to facilitate easy consumption and testing			
PRT-5-18	The Bidder should describe how its proposed Solution will integrate with the RCMP corporate email system in order to ingest as well as send submissions and service requests.	Demonstrated: 10 points Not Demonstrated: 0 points		
Activity and Audit Logging				
PRT-5-19	The Bidder should describe how its proposed Solution will log all User activity in a read-only, immutable Activity Log containing: a. User id b. Activity timestamp c. Activity performed d. Value before editing e. Value After editing.	Maximum 10 points (2 points each)		
PRT-5-20	The Bidder should describe how its proposed Solution would allow a User to record a manual Activity Log entry to record off-line activities such as phone calls or Open Source Searches.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-21	The Bidder should describe how its proposed Solution will log all user access to the system in an immutable Audit Log, including:	Maximum 10 points		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	a. Who logged in b. Login time c. Logout time d. Permissions Granted e. Attempted and Failed login	(2 points each)		
PRT-5-22	The Bidder should describe how its proposed Solution will retain all query search criteria and the subsequent query results in an immutable Query Log.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-23	The Bidder should describe how its proposed Solution maintains all historical versions of a file if it is manipulated during intelligence extraction, language translation or any other analysis activities.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-24	The Bidder should describe how its proposed solution will log all activities performed automatically by the system in an immutable Audit Log.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-25	The Bidder should describe how its proposed Solution will provide search and view capabilities of Activity, Audit and Query logs to authorized NC3 users to based on configurable permissions.	Demonstrated: 10 points Not Demonstrated: 0 points		
Online Text Chat				
PRT-5-26	The Bidder should describe how the proposed Solution will support a secure (Protected B) online Chat/Conference feature including: a. Opening and closing a secure channel to initiate or end a Chat b. Invite Users to a Chat	Maximum 20 points (2 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	c. Allow invited users to join d. Monitor Chat attendance e. Enable Voice f. Enable Video g. Enable 1:1 Chats h. Enable Messaging i. Capture and log Chat content between attendees j. Allow exchange of Files including images			
Document Publishing and Productivity Applications				
PRT-5-27	The Bidder should describe how its proposed Solution supports integration with common word processing tools or appropriate readers/viewers for the purposes of: a. Accessing, reading, and viewing b. Editing c. Spell checking of documents, d. Viewing structured and unstructured data e. Viewing images in native file format.	Maximum 10 points (2 points each)		
PRT-5-28	The Bidder should describe how its proposed Solution is capable of allowing a user to create and send an email (including a secure email) to a cybercrime partner.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-29	The Bidder should describe how its proposed Solution provides "save as" and file conversion capability that will allow for the conversion of a file from one type to another, including: a. MS Word to PDF b. MS Excel to PDF	Maximum 10 points (2 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	c. Email to PDF d. Image to PDF			
PRT-5-30	The Bidder should describe how its proposed Solution provides authorized internal NC3 users or external P3 users with a secure collaboration environment that supports real-time concurrent access, modification, feedback and discussion of Tools, Projects and artifacts including: a. Ability to collaborate on text documents, spreadsheets, PDFs and presentations b. Ability to collaborate on visualization maps or images c. Ability to maintain the history and integrity of prior revisions d. Ability for a User to Screen Share to display and demonstrate tools and artifacts	Maximum 12 points (3 points each)		
Speech to Text, Translation, and OCR				
PRT-5-31	The Bidder should describe how its proposed Solution supports Audio to Text Conversion and Language Translation including: a. Link original audio and text files and all resulting text files to the associated NCS file b. Convert and translate Audio (English and non-English Languages) to English text c. Translate English text to French text or French text to English text d. Translate Non-English Language Text to English text e. Support for multiple non-English or French languages f. Indicate non-native speech in resulting text g. Identify the language(s) being spoken in an audio file h. Identify individual speakers in an audio file	Maximum 16 points (2 points each)		
Identity Management				

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRT-5-32	The Bidder should describe how its proposed Solution provides a user with the ability to manage their password. Password management should comply with RCMP standards including: a. Mandatory password for all users b. Password contains a minimum of 8 characters including a mix of uppercase & lowercase and at least one special character c. Password change must be enforced at first login d. Maximum password lifetime of six (6) months must be enforced e. Users must have the ability to change their password at any time f. Users must be able to re-set a forgotten password at any time g. Forgotten Password recovery process with user questions & answers	Maximum 14 points (2 points each)		
PRT-5-33	The Bidder should describe how its proposed Solution allows an authorized RCMP user to view, create, modify, suspend or reinstate an NC3 or P3 user of the Solution.	Demonstrated: 10 points Not Demonstrated: 0 points		
Usability				
PRT-5-34	The Bidder should describe how its proposed Solution provides an admin user role with the capability to extend and customize application functionality using a low-code or no-code approach, including: a. customizable dashboards b. customizable work queues c. configurable data selection lists d. adding/configuring validation business rules e. adding/configuring report templates f. adding/configuring data entity and attribute data capture templates and screens g. adding/configuring search templates	Maximum 14 points (2 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRT-5-35	The Bidder should describe how its proposed Solution allows configuration without incurring system downtime or new software releases.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-36	The Bidder should describe how its proposed Solution provides a User Interface with meaningful: a. workflow sequences b. information relationships c. field focus d. messages e. consistent look and feel f. screen labels g. consistent navigation and orientation h. user warnings	Maximum 16 points (2 points each)		
PRT-5-37	The Bidder should describe how its proposed Solution provides users with access to context sensitive on-line help.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-38	The Bidder should describe how its proposed Solution eases and standardizes data capture by making use of: a. Searchable data selection lists b. auto-fill controls c. pop-up help / Tool-Tips d. Date Time Picker (Calendar widget) e. Progress Indicators	Maximum 12 points (2 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	f. Undo controls			
PRT-5-39	The Bidder should describe how its proposed Solution makes maximum use of existing data (for example; Client or Partner Directory data) to minimize user data entry (pre-fill and auto-complete) and maximize accuracy.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-40	The Bidder should describe how its proposed Solution allows a user to create a request for assistance.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-41	The Bidder should describe how its proposed Solution is available and accessible to individuals with disabilities, compliant with WCAG 2.0 Accessibility standards.	Demonstrated: 10 points Not Demonstrated: 0 points		
NCS Repository				
PRT-5-42	The Bidder should describe how its proposed Solution is capable of storing data that is received in multiple languages as defined by the ISO language codes listed in alpha-3/ISO 639-2.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-43	The Bidder should describe how its proposed Solution supports metadata standards including: a. Government of Canada's TBS Standard on Metadata (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18909) b. Dublin Core Metadata Element Set (http://www.dublincore.org/) c. Support for modification of the Metadata Element Sets	Maximum 9 points (3 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRT-5-44	The Bidder should describe how its proposed Solution is capable of storing, indexing, and searching on the following data formats: a. Structured data b. Semi-structured c. Unstructured data d. Images e. Video	Maximum 10 points (2 points each)		
PRT-5-45	The Bidder should describe how its proposed Solution protects information and data from unauthorized action and access.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-46	The Bidder should describe how its proposed Solution protects information and data from accidental or deliberate loss and corruption.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-47	The Bidder should describe how its proposed Solution supports Elastic and Scalable data storage capabilities.	Demonstrated: 10 points Not Demonstrated: 0 points		
System Monitoring				
PRT-5-48	The Bidder should describe how its proposed Solution supports monitoring: a. User access (login, logout) b. Database growth and utilization c. Database access d. Error messages	Maximum 14 points (2 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	e. Repeated User Attempts f. Cloud Resource utilization (such as compute, storage, messaging) g. Network traffic			
PRT-5-49	The Bidder should describe how its proposed Solution supports use of RCMP Protected B Cloud tenant's log collection capability to store and manage all logs including: a. Activity logs (Control-plane events on Resource Manager resources) b. Resource logs (Frequent data about the operation of Resource Manager resources in subscription) c. Active Directory reporting (Logs and reports) d. Virtual machines and cloud services (Windows Event Log service and Linux Syslog) e. Storage Analytics (Storage logging, provides metrics data for a storage account) f. Network security group (flow logs, JSON format, shows outbound and inbound flows on a per-rule basis) g. Application insight (Logs, exceptions, and custom diagnostics) h. Process data / security alerts (Security Center alerts, Monitor logs alerts)	Maximum 16 points (2 points each)		
PRT-5-50	The Bidder should describe how its proposed solution supports: a. Administrator notification of system component failure b. Administrator notification of repeated user attempts resulting in error messages	Maximum 10 points (5 points each)		
Non-Functional				
PRT-5-51	The Bidder should describe how its proposed Solution: a. Captures run-time exceptions generated during NCS business transaction processing	Maximum 10 points (2 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	b. Handles dead-letter queue messages generated during NCS business transaction processing c. Documents error handling, including error recovery d. Documents retry policies e. Documents compensation policies			
PRT-5-52	The Bidder should describe how its proposed Solution supports error analysis using message Correlation Ids to facilitate the tracking and logging of events through the system.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-53	The Bidder should describe how its proposed Solution allows system administrators to examine system errors and update each error with a resolution once resolved.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-54	The Bidder should describe how its proposed Solution provides a browser-based client as its user interface that is compatible with: a. Internet Explorer v11 on Windows b. Google Chrome v80 and higher (on Windows, MacOS, iOS Android) c. Microsoft Edge v80 and higher (on Windows, MacOS) d. Microsoft Edge v44 and higher on iOS e. Microsoft Edge v43 and higher on Android f. Firefox v74 and higher (on Windows, MacOS) g. Firefox v23 and higher on iOS h. Firefox v67 and higher on Android i. Safari v12 and higher (on macOS, iOS)	Maximum 18 points (2 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
PRT-5-55	The bidders should describe how its proposed Solution supports responsive design enabling access using any device screen size, including desktop, laptop, tablet, or mobile phone, to provide: a. NCS Query Functionality b. Notification Functionality c. Service Request Functionality d. Data Submission Functionality	Maximum 20 points (5 points each)		
PRT-5-56	The Bidder should describe how its proposed Solution provides: a. A single sign-on capability that allows internal users access to the full scope of their authorized functionality b. A single sign-on capability that allows external partners access to the full scope of their authorized functionality	Maximum 10 points (5 points each)		
PRT-5-57	The Bidder should describe how its proposed Solution supports automatic time out after a configurable time of inactivity, after which time re-authentication by the user is required.	Demonstrated: 10 points Not Demonstrated: 0 points		
PRT-5-58	The Bidder should describe how its proposed Solution auto-tags data as it is ingested including: a. time received stamp b. data provider source c. auditing metadata d. monitoring metadata	Maximum 12 points (3 points each)		
PRT-5-59	The Bidder should describe how its proposed Solution captures and retains data lineage and provenance metadata throughout data	Demonstrated: 10 points		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	transformations and data integration processes in accordance with Government of Canada Standards on Metadata. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18909&section=html	Not Demonstrated: 0 points		
PRT-5-60	The Bidder should describe how its proposed Solution performs: a. Data validation b. Data quality monitoring c. Data cleansing for batch data capture processes d. Data cleansing for real-time data capture processes e. Data cleansing for near-real time data capture processes.	Maximum 10 points (2 points each)		
PRT-5-61	The Bidder should describe how its proposed Solution supports data federation by providing: a. virtual access to structured databases b. virtual access to semi-structured data c. the ability to join data across data sources for real-time access and analysis	Maximum 9 points (3 points each)		
PRT-5-62	The Bidder should describe how its proposed Solution supports query optimization: a. automatically as part of DBMS requests b. manually within an advanced SQL editor	Maximum 6 points (3 points each)		
PRT-5-63	The Bidder should describe how its proposed applications are designed and packaged based on Cloud Native Application best practices including: a. Designed and developed as Cloud Native Applications following 12 factor app methodologies b. The use of Containers of one or more Microservices with parameterized scripts that can be tailored for each target	Maximum 6 points (3 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	environment (for example; User Acceptance, Quality Control and Production)			
PRT-5-64	The Bidder should describe how its proposed Solution follows best practices in the design of its Installation/build scripts including: a. Installation/build scripts in a code readable format that can be deployed as a package to build the solution in the appropriate environment b. Update/patch scripts in a code readable format and in a package format to be deployed as an application update c. Each component to be installed on a different server should have its own build script in a code readable format d. Each release should adhere to the RCMP's code repository requirements and release methodology	Maximum 8 points (2 points each)		
Cloud Performance Efficiency				
PRT-5-65	The Bidder should describe how its proposed Solution achieves and maintains performance efficiency, including: a. Using automated triggers to monitor network performance for unused capacity or degradation, and scale the solution accordingly. b. Using automated triggers to monitor application workload performance for unused capacity or degradation, and scale the solution accordingly. c. Using managed services, to reduce or remove administrative and operational overhead. d. Using a data-driven approach, including periodic load testing to evolve the implementation of the solution to achieve performance efficiency.	Maximum 21 points (3 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
	e. Using different compute solutions for various components where appropriate to improve performance and use resources efficiently. f. Using multiple storage solutions and features where appropriate to improve performance and use resources efficiently. g. Using different database solutions for various subsystems where appropriate to improve performance and use resources efficiently.			
Cloud Cost Efficiency				
PRT-5-66	The Bidder should describe how its proposed Solution achieves and maintains cost efficiency, including: a. Creating an account structure which clearly allocates costs and usage across application workloads. b. Using resource tagging to apply business and organization information to usage and cost. c. Using customized dashboards and analytics to control costs and usage using notifications, controls, and service quotas. d. Monitoring resource usage to detect and correct areas of significant underutilization, including the detection and automatic shut down of unused resources. e. Using on-demand or reserved pricing models where appropriate to minimize resource expenses. f. Using a throttle, buffer, or queue to smooth the demand and serve it with less resources resulting in a lower cost. g. Using a batch service to process a workload asynchronously, at a lower cost.	Maximum 21 points (3 points each)		

PRT No.	Requirement Description	Rating Scale	Score	Reference (Proposal Page No.)
Cloud Operations				
PRT-5-67	The Bidder should describe how its proposed Solution collects the necessary information from components to understand their internal system state and provide effective responses where appropriate, including: a. Implementing change control and resource management from project inception to end-of-life. b. Defining, capturing, and analyzing application workload metrics to gain visibility into workload events so that appropriate action can be taken. c. Defining, capturing, and analyzing DevOps metrics to gain visibility into deployment and operational events so that appropriate action can be taken. d. Enabling the automatic detection of component failures and application workload defects, and the automatic bypassing of these events where possible. e. Enabling automatic rapid identification and recovery from deployment changes that do not have desired outcomes.	Maximum 15 points (3 points each)		
		Technical Capabilities - Total Score ▶	**xx/867**	