Canada Deposit Insurance Corporation
Société d'assurance-dépôts du Canada

REQUEST FOR SUPPLY ARRANGEMENT REFRESH[1]

RFSA 2020-2842 - 2021 REFRESH

1. Title

Information Technology Staff Augmentation and Project Delivery Services

2. Introduction and Supply Arrangement Requirements

1. Following RFSA 2020-2842 issued on October 5, 2020 ("**Initial RFSA**"), the Canada Deposit Insurance Corporation (**"CDIC"**) awarded twenty-nine (29) Supply Arrangements under Service Stream #1: Staff Augmentation Services and seventeen (17) Supply Arrangements under Service Stream #2: Project Delivery Services, the "**Initial Supply Arrangements**". CDIC is seeking to establish additional Supply Arrangements during this annual qualification opportunity ("**2021 Refresh**") as well as during each subsequent annual qualification opportunity, for the provision of Information Technology Staff Augmentation and Project Delivery Services in various resource Roles as identified in Schedule "A" (Statement of Work) for any one or both of the following two (2) Service Streams:

   Service Stream #1: IT Staff Augmentation Services
   Service Stream #2: Project Delivery Services

   on an as and when required basis, for a period of approximately two years, that is from the effective date of the resulting Supply Arrangements to December 14, 2023, as further detailed in Section 14 of the RFSA.

2. CDIC is a federal Crown corporation, with headquarters in Ottawa, and an office in Toronto. CDIC is responsible for providing insurance against the loss of part or all of deposits, and for promoting and otherwise contributing to the stability of the financial system in Canada. These objectives are pursued for the benefit of persons having deposits with CDIC member institutions and in such a manner as will minimize the exposure of CDIC to loss. CDIC is also the resolution authority for CDIC member institutions.

Further information about CDIC can be obtained at www.cdic.ca.

3. Trade Agreements

This RFSA is issued in accordance with the following trade agreements:

Chapter Five (Government Procurement) of the Canadian Free Trade Agreement (CFTA)

[1] The complete and official copy of this RFSA 2020-28422021 Refresh, can be found at no cost at Buyandsell.gc.ca

4. Summary of Key RFSA Dates and Defined Terms

1. The following capitalized terms shall have the following meanings where used in this RFSA, and its incorporated schedules and forms:

Request for Supply Arrangement – 2021 Refresh	
Date of Issuance:	December 9, 2021
Deadline for Suppliers to Submit Questions:	December 22, 2021, at 2:00 p.m., Ottawa local time
Deadline for Response to Suppliers Questions:	January 14, 2022
Proposal Submission Deadline:	January 24, 2022, at 2:00 p.m., Ottawa local time
Proposal Delivery Address:	procurement@cdic.ca
CDIC Contact Person:	Judy Ann Hollander

Key RFSA Dates for subsequent annual qualification opportunities will be available with the annual notice published as described in Section 15 (Open Supply Arrangement).

2. The following additional capitalized terms shall have the following meanings where used in this RFSA, and its incorporated schedules and forms:

"**Engagement**" means a specific body of work that was carried out pursuant to a specific client requirement/need;

"**Financial Offer**" consists of the fillable forms contained in Schedule "D" (Financial Offer) and Appendix "D-1" (Financial Offer for Service Stream #1);

"**IT**" means information technology;

"**IS**" means information systems;

"**Professional Services Agreement**" means the agreement to be entered into by a Supplier with CDIC, for any one or both of the Service Streams (see Schedule "F" (Form of Professional Services Agreement);

"**Project Delivery Services**" means the services described in Service Stream #2, as set out in Schedule "A" (Statement of Work);

"**Proposal**" means the Technical Offer and Financial Offer submitted by a Supplier when applying for the Supply Arrangement under this RFSA;

"**Reference Engagement**" means an Engagement, the details of which are being provided by a Supplier as evidence of the Supplier's technical experience and expertise;

"**Reference Engagement Form**" means the fillable form contained in Appendix "C-2" (Reference Engagement Form);

"**RFSA**" means this Request for Supply Arrangement;

"**Role**" means, for purposes of this RFSA, any one role identified in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles) of this RFSA;

"**Service Category**" means, for purposes of this RFSA, any one service category identified in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles) and/or Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories) of this RFSA;

"**Service Request**" means a document issued by CDIC to an SA Holder(s), that includes instructions and applicable CDIC service requirements, which may result in a Task Authorization. (See Section 4, Service Request Process of Schedule "A" (Statement of Work));

"**Service Stream(s)**" means the service category identified as Service Stream #1: Staff Augmentation Services, and/or Service Stream 2: Project Delivery Services, as described in Schedule "A" (Statement of Work);

"**Service Stream #1**" means the service category identified as Service Stream #1: Staff Augmentation Services, as described in Schedule "A" (Statement of Work);

"**Service Stream #2**" means the service category identified as Service Stream #2: Project Delivery Services, as described in Schedule "A" (Statement of Work);

"**SLA**" means service level agreement;

"**SRA**" means secure remote access;

"**Staff Augmentation Services**" means the services described in Service Stream #1, as described in Schedule "A" (Statement of Work);

"**Supplier**" means an entity submitting a Proposal, or who is considering submitting a Proposal in response to this RFSA;

"**Supply Arrangement**" means an arrangement entered into between a Supplier and CDIC by executing a Professional Services Agreement;

"**Supply Arrangement Holder**" or "**SA Holder**" means a Supplier that has entered into a Professional Services Agreement;

"**Task Authorization"** means the authorization issued by CDIC, following the receipt of an SA Holder's response to a Service Request, authorizing services to be completed under the Supply Arrangement; and

"**Technical Offer**" consists of the fillable forms contained in Schedule "C" (Technical Offer), Appendix "C-1" (Technical Offer Form); and Appendix "C-2" (Reference Engagement Form).

3. Words expressed in the singular include the plural and vice versa.

5. Incorporated Schedules and Appendices

In addition to the main body of this RFSA, the following schedules and appendices are included as part of the RFSA:

Schedule/Appendix	Name
Schedule "A"	Statement of Work
Appendix "A-1"	Service Stream #1: Staff Augmentation Services, Service Categories and Roles
Appendix "A-2"	Service Stream #2: Project Delivery Services, Service Categories
Schedule "B"	Evaluation and Selection Process
Schedule "C"	Technical Offer
Appendix "C-1"	Technical Offer Form
Appendix "C-2"	Reference Engagement Form
Schedule "D"	Financial Offer
Appendix "D-1"	Financial Offer for Service Stream #1
Schedule "E"	Mandatory Proposal Forms
Schedule "F"	Form of Professional Services Agreement

6. Questions and Communications Related to the RFSA Documents

1. Any questions or requests for clarification of the contents of, or interpretation or correction, relating to this RFSA, should:

   i) be made in writing prior to the Deadline for Suppliers to Submit Questions
   ii) be addressed only to the CDIC Contact Person
   iii) list the RFSA number in the subject line; and
   iv) be sent by electronic mail to the Proposal Delivery Address.

2. CDIC will provide the Suppliers with a response to questions no later than the Deadline for Response to Suppliers Questions. CDIC will circulate the responses to questions as written addenda to this RFSA, in the same manner as the RFSA.

3. Any attempt by a Supplier or any of its employees, agents, contractors or any other representatives to contact any person at CDIC other than the CDIC Contact Person, or to contact the CDIC Contact Person regarding this RFSA, other than in writing at the Proposal Delivery Address, may in CDIC's sole and absolute discretion, result in the Supplier's disqualification and the rejection of its Proposal.

4. Nothing in this RFSA limits CDIC's right, in its sole and absolute discretion, for which CDIC shall have no obligation, to communicate with any Supplier regarding any matter in the normal course of business from any contractual relationship for the provision of any other or similar goods or services independently of this RFSA.

5. It is the sole responsibility of a Supplier to avail itself of any information it may require, ask any questions, or obtain any clarification of the requirements or other matters in this RFSA, and make its own investigations, projections and conclusions prior to submitting a Proposal.

7. Proposal Delivery

1. Proposals must be received in electronic format at the Proposal Delivery Address no later than the Proposal Submission Deadline, with the time of delivery confirmed by a CDIC authorized representative. It is the Supplier's responsibility to ensure that the Proposal is delivered by the Proposal Submission Deadline to the Proposal Delivery Address. The time of delivery shall be the time the email is received in the inbox of the email address provided as the Proposal Delivery Address.

2. Proposals received after the Proposal Submission Deadline may be deemed to be non-compliant and may be returned to the sender. CDIC may, in its sole and absolute discretion, accept a Proposal delivered to the Proposal Delivery Address after the Proposal Submission Deadline if CDIC deems it to be in CDIC's best interests, and the Supplier demonstrates to CDIC's satisfaction that:

   i) the Proposal would have been delivered to the Proposal Delivery Address by no later than the Proposal Submission Deadline but for circumstances beyond the Supplier's control; and
   ii) CDIC's acceptance of the Proposal would not otherwise confer a substantive advantage on the Supplier.

3. CDIC may only accept Proposals submitted to the Proposal Delivery Address. Proposals submitted by another means or at any other physical location (as applicable) may be deemed by CDIC to be non-compliant and rejected.

4. Suppliers may, in writing, revoke and re-submit a Proposal at any time up to the Proposal Submission Deadline. Suppliers may, in writing, revoke a Proposal at any time (even after the Proposal Submission Deadline).

8. Proposal Format

1. Proposals are to be submitted in either English or French to the Proposal Delivery Address , as follows:

    i) in Adobe Reader format (.pdf); and

    ii) arranged so that:

    a) the "**Technical Offer**", responding to the technical requirements set out in Schedule "C" (Technical Offer), Appendix "C-1" (Technical Offer Form), and all Appendix "C-2" (Reference Engagement Form(s)); and

    b) the "**Financial Offer**", responding to the financial requirements set out in Schedule "D" (Financial Offer) and if applicable Appendix "D-1" (Financial Offer for Service Stream #1)

    shall be submitted in two separate attachments to the email.

It is possible due to file size that the Proposal may not be received. The maximum file size which CDIC is able to receive via email is 20 MB. It is highly recommended to contact the CDIC Contact Person by a separate email to the Proposal Delivery Address to advise that the Proposal has been sent and confirm CDIC's receipt.

---

9. Proposal Requirements and Required Documents

1. Suppliers may submit Proposals for any one or both of the Service Streams.

2. Suppliers must comply with all requirements of this RFSA, including those identified as "must" or "shall", including, but not limited to, the requirement to:

    i) submit information in support of each Rated Requirement listed in Appendix "C-1" (Technical Offer Form) and Appendix "C-2" (Reference Engagement Form);
    ii) comply with all requirements under Schedule "D" (Financial Offer); and
    iii) submit a Technical Offer and a Financial Offer (including all forms listed in Schedule "E" (Mandatory Proposal Forms)), completed as required.

3. Where a Supplier fails to include any of the required information or documents in its Proposal, CDIC may, in CDIC's sole and absolute discretion (but provided that it treats all Suppliers in the same manner):

    i) require the submission of such information or documents within a prescribed timeframe satisfactory to CDIC; and
    ii) reject or refuse to consider any Proposal from a Supplier who fails to comply with any such submission requirement.

---

10. Evaluation and Selection

Proposals will be evaluated in accordance with the competitive process set out in Schedule "B" (Evaluation and Selection Process), leading to the selection of successful Suppliers, each to enter into a Professional Services Agreement with CDIC to become SA Holders.

The successful Suppliers will be notified via email to the contact person at the email address provided by the Supplier in Schedule "C" (Technical Offer).

Following the issuance of Supply Arrangements with successful Supplier resulting from this RFSA, CDIC will inform unsuccessful Suppliers of the results of their Proposals.

---

11. CDIC's Reserved Rights

Notwithstanding anything to the contrary in this RFSA, CDIC reserves the right in its sole and absolute discretion to exercise any or all of the following rights, alone or in combination with each other, to:

1. Evaluate or accept Proposals:

   i) which in CDIC's sole and absolute discretion substantially comply with the requirements of this RFSA; or
   ii) in whole or in part without negotiations.

2. Enter into negotiations with:

   i) any or all Suppliers on any or all aspects of their Proposal, to ensure CDIC's operational requirements are met and to promote best value; or
   ii) any or all Suppliers, or any prospective persons or entities capable of delivering the required services but who may not have submitted a Proposal in response to this RFSA in the event, in CDIC's sole and absolute discretion, no Proposals meet the requirements of this RFSA.

3. Conduct a best and final Proposal process:

   i) with any or all Suppliers, in which Suppliers are invited to revise their financial offers in circumstances where CDIC deems it appropriate, in CDIC's sole and absolute discretion.

4. Cancel, modify, re-issue or suspend:

   i) any aspect of this RFSA, in whole or in part, at any time, for any reason;
   ii) the schedule for this RFSA, including without limitation the Proposal Submission Deadline stated above and any other activity or date stipulated in this RFSA, in whole or in part, at any time, for any reason; or
   iii) this RFSA in its current or modified form and invite Proposals from only the Suppliers who submitted Proposals in response to this RFSA, where to do so is deemed, in CDIC's sole and absolute discretion, to be in CDIC's best interests.

5. Seek clarification, validate or take into account:

   i) independently or with the help of the Suppliers, any or all information provided by the Supplier with respect to this RFSA and, for this purpose, disclose any or all information provided by the Supplier to a third party, subject to CDIC obtaining appropriate assurances of confidentiality from those third parties.

6. Reject or refuse to consider any Proposal:

   i) if, in CDIC's sole and absolute discretion, it fails in any material respect to comply with the requirements of this RFSA;
   ii) containing false, misleading or misrepresented information;
   iii) in the event any matter causes or is likely to cause, in CDIC's sole and absolute discretion, a conflict of interest in relation to the selection of any Proposal;
   iv) from a Supplier who colludes with one or more other Suppliers in the preparation of any Proposal;
   v) from a Supplier who fails to cooperate with CDIC in any attempt by CDIC to clarify or validate any information provided by the Supplier or who fails to provide accurate and complete documentation as directed by CDIC;
   vi) from a Supplier against whom economic sanctions have been imposed by the Government of Canada;
   vii) from a Supplier with whom CDIC has previously terminated an agreement for any reason;

viii) from a Supplier failing to have the capacity to contract with CDIC, or Her Majesty, or both; or
ix) if deemed by CDIC, in its sole and absolute discretion, as necessary to safeguard Canada's security interests or if the Supplier is prohibited from receiving any benefits under an agreement between Her Majesty and any other person by virtue of Section 750(3) of the *Criminal Code of Canada*.

7. Award:

   i) Professional Services Agreements in connection with Service Stream #1 and Service Stream #2, as described in Schedule "A" (Statement of Work). By entering into a Professional Services Agreement, CDIC does not guarantee that any requests for services will actually be awarded to an SA Holder; and
   ii) one or more Suppliers with Professional Services Agreements for more than one Service Stream, as described in Schedule "A" (Statement of Work).

8. Waive:

   i) irregularities, informalities, non-conformity, non-compliance, omissions and defects in any Proposal where, in CDIC's sole and absolute discretion, they do not materially affect the ability of the Supplier to provide the goods or services required by this RFSA.

The exercise of any of the above rights or sub-rights of CDIC shall not be a waiver or limit the right of CDIC to exercise any other rights.

---

12. Limitation of Liability

1. By submitting a Proposal, the Supplier acknowledges and agrees to the requirements of this Section 12.

2. The Supplier acknowledges and agrees that in no event shall CDIC, its employees, officers, directors, consultants or advisors be liable or responsible for:

   i) any damages, including without limitation direct, indirect, consequential, incidental, general, special or exemplary damages, any economic losses, any lost profits, opportunities, expenses, costs or any other losses arising out of, in connection with, or in any way related to, any Supplier's participation in this RFSA or any acts, omissions or errors, including negligence of CDIC, its employees, officers, directors, consultants and advisors; or
   ii) any actions of any Supplier in relation to CDIC, or another Supplier, or any third party, in receiving and responding to this RFSA.

3. Without limiting the above, expenses or costs incurred by any Supplier in any way related to or associated with this RFSA, including without limitation the preparation, submission or evaluation of Proposals, the provision of information to CDIC or CDIC's authorized representative for a determination of any Supplier's technical, managerial or financial capabilities, any expenses related to travel, and the satisfaction, fulfillment or completion of any conditions precedent to any agreement with CDIC to deliver the goods and services required by this RFSA, are a Supplier's sole responsibility and may not be charged to CDIC in any way.

4. Without limiting any rights CDIC may reserve elsewhere in this RFSA or may have otherwise at law, CDIC may, in its sole and absolute discretion, elect to exercise its sole and absolute discretion pursuant to this RFSA, without any liability or obligation to any Supplier.

5. If any Supplier is determined by a court or trade tribunal of competent jurisdiction to be entitled to compensation arising from this RFSA or from the actions of CDIC, its employees, officers, directors, consultants or advisors in relation to this RFSA,

including without limitation any exercise of CDIC's sole and absolute discretion, the Supplier expressly acknowledges and agrees by submitting a Proposal that the total maximum compensation for, without limitation, any and all damages, economic losses, profits, opportunities, expenses, costs, or other losses, either individually or cumulatively, is limited to one thousand dollars ($1,000.00 CAD).

---

13. Governing Law

This RFSA is governed by and construed in accordance with the laws in force in the Province of Ontario, Canada, and, subject to the jurisdiction of the Canadian International Trade Tribunal, Ontario courts have exclusive jurisdiction to hear any disputes under this RFSA.

---

14. Resulting Agreements and Term of Agreement

1. CDIC intends to award agreements based on Schedule "F" (Form of Professional Services Agreement), covering Service Stream #1, and/or Service Stream #2, each for a term of approximately two years, from the effective date of the resulting Supply Arrangement(s) to December 14, 2023, plus, at CDIC's sole discretion, two (2) options to extend for a one (1)-year term, to expire no later than December 14, 2025, if exercised.

   Each such Professional Services Agreement will include:

   i) the applicable portion(s) of the Statement of Work, attached to this RFSA as Schedule "A" (Statement of Work);
   ii) any other RFSA document CDIC deems appropriate to include as part of the resulting agreement(s); and
   iii) the applicable documents submitted with the successful Proposal.

2. CDIC intends to have Professional Services Agreements in place with successful Suppliers by March 2022 for this RFSA 2021 Refresh. Successful Suppliers will be expected to enter into Professional Services Agreements with CDIC within fifteen (15) business days of being notified of having been selected as a successful Supplier.

3. Once CDIC has entered into a Professional Services Agreement with a successful Supplier, CDIC may, in its absolute discretion, begin requesting services from any such firm, whether or not any Professional Services Agreements have yet been entered into with other successful Suppliers.

---

15. Open Supply Arrangement

It is currently CDIC's intention that the Supply Arrangement established under this RFSA will be open during the term of the Supply Arrangement to allow, pursuant to the terms and conditions of a separate request for Supply Arrangement:

i) additional firms to be selected as SA Holders under the Supply Arrangement for any one or both of the Service Streams and/or Service Categories and/or Roles described in this RSFA; and/or
ii) qualified SA Holders to be selected to provide services in service streams and/or categories of resources for which they were not previously qualified under this RSFA; and/or
iii) firms to be selected as SA Holders under this Supply Arrangement for new service streams and/or categories of resources that may be added by CDIC in the future.

A notice will be published once a year on www.buyandsell.gc.ca (or such other electronic tendering service utilized at the relevant time) inviting interested suppliers to submit proposals for consideration and potential award of a Supply Arrangement.

16. No Guarantee of Volume of Work or Exclusivity of Contract

CDIC makes no guarantee of the value or volume of work SA Holders may receive through the Supply Arrangement. The value and volume of Services, (if any), acquired will depend on a variety of factors including annual budgetary approvals.

The Professional Services Agreement executed with SA Holders will not be exclusive contracts for the provision of the described Services. CDIC may contract with others for the same or similar services to those described in this RFSA or may obtain the same or similar services internally.

---

17. Debriefing

After notification of the results of the RFSA process, Suppliers may request a debriefing. Suppliers should make the request to the CDIC Contact Person within fifteen (15) business days of receipt of the notification. The debriefing may be in writing, by telephone or by video conference. The intent of the debriefing information session is to aid Suppliers in understanding why their Proposal was not selected. Any debriefing provided is not for the purpose of providing an opportunity to challenge the procurement process.

---

18. Disclaimer

CDIC makes no representation or warranty as to the accuracy or completeness of any information provided by it in connection with this RFSA and disclaims all express and implied representations, warranties, and conditions in connection with this RFSA. Suppliers should make their own investigations, projections and conclusions. They should consult their own advisors to verify independently the information contained in this RFSA and to obtain any additional information that they may require, prior to submitting a Proposal.

---

19. No Assumptions or Conditions

All prices contained in the Appendix "D-1" (Financial Offer for Service Stream #1) shall be fixed prices and not subject to change after award of an agreement due to incorrect assumptions or conditions made by any Supplier, whether or not these conditions or assumptions are stated in the Supplier's Proposal. To the extent a Supplier requires additional information in order to provide fixed prices; the Supplier should seek clarification from CDIC, as described in Section 6, Questions and Communications Related to the RFSA Documents, as part of this RFSA process.

---

20. General

1. In the event of any discrepancy, inconsistency or conflict between the wording of the English or French version of this RFSA, or any related documents, the wording of the English version shall prevail.

2. CDIC agrees to keep in confidence any information contained in a Proposal that is clearly marked "confidential". Notwithstanding the foregoing, the submission of a Proposal by a Supplier constitutes an acknowledgement by that Supplier that CDIC is subject to the *Access to Information Act* (Canada), as amended from time to time, and that, as a consequence, CDIC may be required to disclose certain information contained in its records pursuant to a request for access made under that Act.

3. CDIC requires any persons supplying services to or performing any work for CDIC to conduct their affairs to avoid any conflict of interest. A conflict of interest includes any situation where a Supplier has or may have an unfair advantage or where other commitments, relationships or interests could or could be seen to compromise a Supplier's performance of its obligations to CDIC. To the extent that a Supplier may be in a conflict of interest, that Supplier must include a description of such conflict of interest in its Proposal.

4. If CDIC is of the belief that a Supplier may be in a conflict of interest, CDIC may disqualify the Proposal submitted by the Supplier or terminate any agreement with that Supplier pursuant to this RFSA.

21. Not a Tender, No "Contract A / Contract B"

This RFSA is not an offer to enter into either a bidding contract (often referred to as "Contract A") or an agreement to acquire goods or services from the Supplier (often referred to as "Contract B"). Neither this RFSA nor a Supplier's Proposal shall create any contractual rights or obligations whatsoever on any of CDIC or any Supplier, save and except related to limitation of liability.

Supplier Proposals are revocable by Suppliers; however, CDIC is under no obligation to continue to evaluate or consider any Proposal that the Supplier seeks to modify following the Proposal Submission Deadline (including any change in pricing that is adverse to CDIC). Proposals and related information about Suppliers will be assessed during the evaluation of Proposals and accordingly, misleading or incomplete information, including withdrawn or altered Proposal information or pricing, could adversely impact any such evaluation (or result in CDIC revisiting that evaluation) and may result in disqualification (in CDIC's sole discretion).

[END OF MAIN RFSA BODY]

Schedule "A"

Statement of Work

1. BACKGROUND

CDIC was established in 1967 by the *Canada Deposit Insurance Corporation Act* (Canada). It is a federal Crown corporation named in Part I of Schedule III to the *Financial Administration Act* (Canada). The Corporation reports to Parliament through the Minister of Finance.

CDIC is responsible for providing insurance against the loss of part or all of deposits, and for promoting and otherwise contributing to the stability of the financial system in Canada. These objectives are pursued for the benefit of persons having deposits with CDIC member institutions and in such a manner as will minimize the exposure of CDIC to loss. CDIC is also the resolution authority for CDIC member institutions.

In furtherance of its statutory mandate, CDIC performs certain core functions with respect to member institutions which include:

a) Validation and continued testing of member institution compliance with data standards and system requirements

b) Calculation of deposit liability and collection of insurance premiums from member institutions to provide an adequate level of insurance protection for Canadians' eligible deposits

c) Proactive and continued risk monitoring and, where necessary, timely intervention at member institutions; and

d) Assessing, determining and administering appropriate payouts of eligible insured funds to depositors, where appropriate.

In support of its mandate, CDIC's information systems continue to evolve and increase in complexity in order to support CDIC's business requirements. As CDIC's reliance on technology continues to expand, investments to ensure the stability and integrity of systems and security of information will persist. As such, CDIC is continuing to improve its IS service delivery model, ensuring that IS resources are strategically aligned with operational requirements and deliver efficiently and effectively.

2. OBJECTIVES

This RFSA is an invitation issued by CDIC to prospective Suppliers to provide Proposals for the delivery of Staff Augmentation and Project Delivery Services (the Service Streams) as further described in, and in accordance with, this RFSA.

This RFSA will establish a multi-year Supply Arrangement vehicle with experienced and qualified firms (SA Holders), capable of delivering the services of qualified resources, as described herein.

3. SERVICE STREAMS

The Supply Arrangement vehicle will incorporate two (2) Service Streams with services to be requested on an as and when required basis through a Service Request.

In order for a Supplier to be qualified to become an SA Holder on the Supply Arrangement, the Supplier must qualify to provide Services in one or both of the following two (2) Service Streams by qualifying for at least one Service Category, (as set out in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles) and Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories)), under the Service Stream(s), for which the Supplier wishes to qualify:

SERVICE STREAMS
Service Stream #1: Staff Augmentation Services
Service Stream #2: Project Delivery Services

All Proposals submitted in response to this RFSA will be evaluated in a competitive process leading to the selection of Suppliers, to become SA Holders capable of delivering the Services, each to enter into a Professional Services Agreement.

3.1. Service Stream #1: Staff Augmentation Services

a) **Requirements and services**

CDIC's IS department must continually support CDIC's day-to-day operations. Staff Augmentation Services are supplementary to CDIC's internal IS staff to cover temporary absence of CDIC resources (e.g., due to leave) or to provide targeted support to on-going services or special projects where additional resources may be required.

CDIC invites prospective suppliers to submit Proposals to supply staff augmentation services in forty-one (41) resource Roles across eleven (11) Service Categories of the Initial RFSA, as further identified and described in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles).

For this RFSA 2021 Refresh, eight (8) additional roles, as further identified and described in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles) are being added.

Resources will be required in one, some, or all of junior (level 1), intermediate (level 2), and/or senior (level 3) experience levels, as indicated herein and as further specified in any resultant Service Request.

Specific required deliverables and scopes of work will be specified in any resultant Service Request. Notwithstanding, deliverables will generally align with the job activities / responsibilities provided Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles) which contains a detailed description of each resource Role.

b) **Service Categories and Roles**

The Service Categories and Roles of resources that CDIC may request under Service Stream #1 include those listed in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles), attached to and forming part of this Schedule "A" (Statement of Work). Suppliers must provide in their Proposals, pricing rates for each of the Roles they intend on offering as part of their Proposal for Service Stream #1. For clarity, such pricing will not be evaluated, but will form part of any Professional Services Agreement entered into with an SA Holder.

3.2. Service Stream #2: Project Delivery Services

a) **Requirements and Services**

As CDIC continues to evolve and grow, the pressure to expand IT functionality increases. Projects are designated to address technology or business changes to support and sustain the operation and future growth of CDIC. Presently, the number of projects exceed the capacity of current staffing levels. Accordingly, CDIC is seeking qualified Suppliers to provide full project delivery support to achieve organizational goals and objectives across seven (7) Service Categories, as further identified and described in Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories).

No additional Service Categories are applicable to this RFSA 2021 Refresh.

It is anticipated that CDIC will undertake approximately twelve (12) projects per year under the Supply Arrangement framework. Notwithstanding, projects will generally align with the categories identified in Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories). Some of the projects may comprise routine, ongoing activities while others may be required on a recurrent or ad-hoc basis.

Key considerations for project delivery process:

i. CDIC takes a collaborative approach to project delivery. It is anticipated that SA Holders will work alongside CDIC to define the project approach, methodology, pricing and assignment of supporting resource(s) in compliance with CDIC's overall policies and procedures.

ii. At present, most of CDIC's projects are run typically using agile methodology for the planning, design, development, testing and deployment of projects, although other development methodologies may be used as appropriate. CDIC is seeking Suppliers capable of incorporating agile methodologies into the project delivery life cycle to deal with on-going changes in the business and external environment.

iii. Projects may require extensive project management throughout all phases of the project life cycle with application of appropriate project management techniques on an as and when required basis.

b) **Service Categories**

The Service Categories that CDIC may request under Service Stream #2 (Project Delivery Services) include, but are not limited to, those listed in Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories), attached to and forming part of this Schedule "A" (Statement of Work).

4. SERVICE REQUEST PROCESS

All services to be completed under the Supply Arrangement will result from a Service Request process. Upon written acceptance by CDIC of an SA Holder's response to a Service Request, the SA Holder will be authorized by Task Authorization to proceed with the delivery of Services in accordance with the agreed upon Service Request response.

The current Service Request process is generally described below for information purposes only, and may be amended from time to time, at CDIC's sole discretion.

CDIC will issue a Service Request to one or more SA Holders describing the requirements of a specific engagement, including the required timeframe to respond and requesting the SA Holder to propose appropriate personnel to provide the Services. The number of SA Holders invited to bid on an engagement is determined by the dollar value of the engagement.

Only SA Holders on the Supply Arrangement will be notified of any engagements, be issued Service Requests, and be eligible to respond to Service Requests. If an SA Holder responds to a Service Request, it will do so at no charge to the CDIC.

The Service Requests may include, but are not limited to, the following for each respective Service Stream as required:

a) Service Stream #1: Staff Augmentation Services:

i. A list of required resource Roles, levels, and number of resources required
ii. The minimum qualification requirements for the required resource Role(s)
iii. The overall scope of work and any tasks specific to any resource Role(s)

iv. The schedule and duration of the work assignment
v. Any Service Request assignment specific SLAs
vi. Any technology requirements specific to the work
vii. Deliverable requirements
viii. Any resource or technological security requirements above the minimum; and
ix. Any other requirements related to the Services, including vaccination requirements, as applicable.

b) Service Stream #2: Project Delivery Services:

i. The overall scope of work and any required tasks
ii. Any Service Request assignment specific SLAs
iii. Any additional technology requirements specific to the Services
iv. Deliverable requirements
v. Any resource or technological security requirements above the minimum
vi. Any other requirements related to the Services including vaccination requirements, as applicable, and
vii. Roles and responsibilities of CDIC resources, if applicable.

The SA Holder must include in its response to the Service Request, the names and resumes of each resource that it proposes. Reference checks may be conducted on the resource(s) proposed and such checks may be with references other than those listed in the resource's resume or in the SA Holder's response to the Service Request. Any other information requested in the Service Request should also be included in the SA Holder's response to the Service Request. SA Holders will respond to the Service Request with submissions that are then evaluated by CDIC, who will select the most suitable SA Holder for its engagement through the issuance of a written Task Authorization.

5. REPORTING

SA Holders may be requested to provide a monthly report to CDIC on all active Task Authorizations including, but not limited to:

a) Status of work and any pending end dates, including all related applicable Task Authorization reference numbers provided by CDIC
b) The name(s), role(s) and overall volume of resources engaged, and effort expended including timesheets
c) Performance under any (if applicable) vendor performance management framework, including monitoring of resource turnover, and any issues and resolutions required
d) An invoice including a summary of the services provided in the preceding month, and the related purchase order number(s) and Task Authorizations number(s)
e) For Task Authorizations that include a task/engagement specific SLA with CDIC, the SA Holder should report on its delivery of services against the identified SLA(s) within its monthly report.

6. LANGUAGE REQUIREMENTS

SA Holders must be able to provide resources who are proficient in English, at a minimum, and in some cases may be required to provide bilingual resources who are proficient in English and French. When CDIC advises of the need to fill a Role for a respective service stream, CDIC will specify the language requirement for the assignment at the time of issuance of the Service Request.

7. LOCATION OF WORK

As the COVID-19 situation continues to evolve, future determination as to whether the work must be performed on-site or off-site will be specified in the Service Request Where CDIC determines that the work must be performed at CDIC's offices, CDIC will advise whether the work is to be performed at its office in Ottawa, Ontario, or its office in Toronto, Ontario. In either case, CDIC is not responsible for any travel or accommodation costs.

Beyond the pandemic, in exceptional circumstances for services not requiring access to highly sensitive information, data or applications, or otherwise at CDIC's discretion, CDIC may allow for remote/off-site work by providing the qualified resource with an SRA token/password.

Deployed resources must use CDIC equipment to provide services on-site at CDIC premises. No personal information or other confidential information may leave CDIC premises or be transferred to any third party or transferred out of Canada.

NOTE TO SUPPLIERS: CDIC will accept a Supplier that has a parent, subsidiary or other related company operating in a location outside of Canada, provided that those related companies are not performing the Services outlined in the resulting Professional Services Agreement and do not have access to CDIC confidential information marked as "Protected B".

Suppliers may back-up information on servers outside of Canada except where the information is classified as "Protected B". "Protected B" information must remain within Canada.

8. WORK HOURS

Specific work hours will be included with any resultant Task Authorization. Notwithstanding, service requirements will generally be within the following timeframe, which is applicable to both the Ottawa and Toronto locations:

a) **Primary Hours:** 7-hour day (or portion thereof), between the hours of 8 a.m. to 6 p.m., Monday to Friday (except Statutory Holidays); and

b) **Off-Hours:** CDIC anticipates that there may be some requirements for service delivery outside of the primary hours described above. Such requirements may arise as a result of critical project deadlines, requirement for system patches, or other requirements. CDIC will provide reasonable advance notice to the SA Holder of any such requirement. Any service delivery authorized by CDIC to be completed outside of the primary hours described above will be paid on the basis of hours actually worked, in accordance with the SA Holder's rate(s) for resource Roles (as accepted by CDIC); with no allowance for over-time.

9. SECURITY CLEARANCE

SA Holders must be able to supply and assign resources who are legally entitled to work in Canada, and that possess a valid security clearance granted by the Industrial Security Program of Public Works and Government Services Canada at the Reliability Status level, at a minimum, for work under any resultant Service Request.

CDIC may require higher security levels (e.g., Secret) for services to be rendered under a Service Request, and such additional security requirements will be indicated at the time of issuance of the Service Request.

CDIC will validate/confirm that all resources assigned to provide services under a Service Request possess the applicable security level required prior to authorization of any services to be rendered under a Service Request. Resources not currently in possession of a security clearance will need to obtain the required security clearance prior to commencement of any services.

10. RESOURCE AVAILABILITY AND SUBSTITUTION

SA Holders should ensure that resources proposed and deployed in response to any issued Task Authorization should remain available for the duration of the period stipulated in the Task Authorization, unless the resource becomes unavailable due to circumstances beyond the SA Holder's control (such as, but not limited to, illness, termination of employment with the SA Holder, or compassionate leave).

For short-term assignments or engagements (typically less than ninety (90) days), as identified within a Task Authorization, no resource substitution by the SA Holder may be permitted without CDIC's prior consent or approval.

For longer-term assignments or engagements (typically ninety (90) days or more), as identified within a Task Authorization, a maximum number of qualified resource substitutions may be permitted by CDIC as identified in the Task Authorization, dependent upon duration of the engagement.

CDIC reserves the right to require the SA Holder to replace any deployed resource(s) should an individual not meet CDIC's qualification requirements and performance expectations.

11. VENDOR PERFORMANCE MANAGEMENT

CDIC is intending to enhance the vendor performance management process. This process may consist of new metrics, tools, reports, processes and remedies designed to effectively and efficiently measure, report on and manage the level and quality of service being provided to CDIC.

SA Holders will be expected to comply with the vendor performance management guidelines that may be issued from time to time.

Should changes to performance management reporting and processes be implemented during the term of the Supply Arrangement, the SA Holders shall cooperate fully with CDIC in providing the information required and adapting existing processes to reflect the changes resulting from the implementation of these enhancements.

[END OF SCHEDULE "A" (STATEMENT OF WORK)]

Appendix "A-1"

Service Stream #1: Staff Augmentation Services,
Service Categories and Roles

Projects undertaken by CDIC may require either an individual resource or a team of resources to work with CDIC. CDIC may require resources to have additional skills or subject matter expertise for specific engagements.

The following three (3) levels apply to all Roles in this RFSA (unless otherwise specified):

Level 1: Resource with basic/junior experience in successfully performing the Role.
Level 2: Resource with intermediate experience in successfully performing the Role.
Level 3: Resource with advanced experience in successfully performing the Role.

The following is a list of the eleven (11) Service Categories for Service Stream #1: Staff Augmentation Services applicable to the Initial RFSA and to this RFSA 2021 Refresh.

#	Service Category
1	Advisory Services
2	Project Management
3	Cyber Security
4	Enterprise Technology
5	Technical Support
6	SharePoint Support
7	Salesforce Support
8	Alteryx Support
9	Agile Application Delivery
10	Application Development
11	Business Intelligence and Analytics

A. Additional Roles for the RFSA 2021 Refresh

The following is a list of eight (8) additional Roles for Service Stream #1: Staff Augmentation Services, applicable to this RFSA 2021 Refresh, and are defined in Section C below.

Role #	Service Category #2 - Project Management
42	IT Service Manager

Role #	Service Category #3 - Cyber security
43	Cyber Forensics Specialist
44	Security Engineer (Application/Network)
45	SOC Analyst
46	SOC Lead/Manager
47	Cloud Security Specialist
48	Security Administrator
49	Governance Risk and Compliance Analyst

B. Roles for the Initial RFSA

The following is a list of the forty-one (41) Roles for Service Stream #1: Staff Augmentation Services, applicable to the Initial RFSA, and are defined in Section D below.

Role #	Service Category #1 - Advisory Services
1	IT Executive Strategic Advisor
2	Data Strategy Advisor

Role #	Service Category #2 - Project Management
3	Project Management Office Lead
4	Project Manager
5	Project Administrator / Coordinator

Role #	Service Category #3 - Cyber security
6	Security Analyst
7	Application Security Administrator
8	IT Security Architect
9	Ethical / White Hat Hacker (or Penetration Tester)
10	Azure Security Architect
11	Azure Security Administrator

Role #	Service Category #4 - Enterprise Technology
12	Storage Administrator / Virtualization Architect
13	Systems Architect (Network, Data, Applications)
14	Azure Architect
15	Azure Administrator
16	Azure Data Base Administrator
17	Webmaster

Role #	Service Category #5 - Technical Support
18	Application Support Specialist
19	Deskside Technical Support Analyst
20	Service Desk Analyst
21	IT Service Management Specialist
22	Security Incident Responder
23	Infrastructure Operations and Support
24	Technical Writer / Trainer / Courseware Author (Developer)

Role #	Service Category #6 - SharePoint Support
25	SharePoint Online Administrator
26	SharePoint Online Architect
27	SharePoint Online Developer

Role #	Service Category #7 - Salesforce Support
28	Salesforce Developer
29	Salesforce Tester
30	Salesforce Administrator

Role #	Service Category #8 - Alteryx Support
31	Alteryx Developer

Role #	Service Category #9 - Agile Application Delivery
32	Scrum Master
33	Agile Team Coach

Role #	Service Category # 10 - Application Development
34	Solution Architect
35	Business Analyst
36	Application Developer
37	Azure Cloud Application Developer
38	Quality Assurance (QA) Tester

Role #	Service Category #11 - Business Intelligence and Analytics
39	Business Intelligence Developer
40	Data Architect
41	Data Scientist

C. Description of Additional Roles for the RFSA 2021 Refresh

1. <u>The following is the specific description for the additional Role in Service Category #2 – Project Management Services.</u>

Role #42 – IT Service Manager
Responsibilities:
a) Establishes the process for change management and ensures that each change follows the complete procedure to ensure minimum disruption to IT services. b) Evaluates all requests for change (RFCs) to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. c) Ensures that changes are logged, prioritized, categorized, assessed, authorized, planned, and scheduled, and are introduced in a controlled and coordinated manner. d) Liaises with all necessary parties to coordinate change building, testing, and implementation, in accordance with schedules. e) Carefully manages emergency changes to minimize further incidents and make sure the change is controlled and takes place securely. Verifies that emergency changes are appropriately assessed and authorized after the change. f) Maintains a tracking and reporting system to document rejected changes, communicates the status of approved and in-process changes, and completes changes. g) Makes certain that approved changes are implemented as planned and ensures that they have met their objectives. Refers back any changes that have been backed out of and have failed. h) Whenever changes are implemented, updates the solution and user documentation and the procedures affected by the change accordingly. i) Analyzes change records to determine any trends. j) Closes RFCs. k) Produces regular management reports. l) Onboarding/Offboarding users m) Scheduling CAB meetings and taking meeting minutes n) Coordinating changes between different teams (TS/Cyber/SD/IG/Dev/Corp app/vendors) and following up o) Sending communications to the impacted stakeholders and keep track of the freeze calendar (i.e., Board meetings) p) Documenting and coordinate incidents q) Developing root cause analysis documentation and reporting following incidents r) Working closely with Internal audit teams to ensure compliance s) Assist on the Asset Inventory Management
Minimum Qualification:
a) College diploma or university degree in the field of computer science and/or systems administration and/or equivalent work experience. b) Certifications in ITIL (Information Technology Infrastructure Library)

2. <u>The following is the specific description for the additional Roles in Service Category #3 – Cyber Security.</u>

Role #43 – Cyber Forensics Specialist
Responsibilities:
a) Conduct deep security analysis on Windows and Unix computer systems b) Conduct deep security assessments in cloud environments, especially Azure c) Complete imaging systems under investigation in the cloud for investigations d) Manage full control of evidence life cycle e) Develop policy and technical procedures f) Forensic imaging and collection of electronic data g) Initial review and culling of data for E-Discovery matters h) Analysis of digital media and subsequent reporting of findings i) Data recovery j) Assist in investigations with information technology (“IT”) components k) Securing of digital evidence with the use of disk imaging techniques and preserving chain of custody l) Recovery and analysis of digital evidence m) Configure, test and maintain forensic support tools in a forensic laboratory environment n) Provide advice to team members and clients on proper data recovery steps and procedures o) Develop links within the organization that can contribute to thought leadership p) Build and maintain excellent relationships with existing and target client organizations q) Develop excellent relationships with colleagues in other areas of the organization r) Document, report and present findings to Senior Management
Minimum Qualification:
a) Bachelors or Diploma in Computer Science, IT, or related field or equivalent work experience. b) 2-5 years’ experience practicing computer/digital forensic investigations, eDiscovery, investigation and support work c) Certification in one or more of the following; CISSP (Certified Information Systems Security Professional); CCE (Certified Computer Examiner); CFCE (Certified Forensic Computer Examiner); CHFI (Computer Hacking Forensic Investigator); GCFA (GIAC Forensic Analyst)

Role #44 – Security Engineer (Application/Network)
Responsibilities:
a) Provision of subject matter expertise and point of reference for matters involving information security, including best practice, controls, technologies, human factors, physical and operational security. b) Review, suggest, and implement improvements for security practices. c) Evaluate complex business and technical requirements, and then communicate inherent security risks and remediation recommendations to technical and non-technical business owners. d) Lead the architecture, design, implementation, support, evaluation and documentation of security-focused tools and services. e) Perform vulnerability assessments including pentesting the CDIC network, hosts and applications. f) Development of logic (including rules and signatures) to mitigate the risk of vulnerabilities. g) Stay current on emerging security threats, vulnerabilities and controls. h) Provide leadership and innovation in the design and implementation of security solutions and controls. i) Provide critical feedback to security solution providers and guidance in the development of product enhancements and features. j) Intermediate or advanced knowledge in securing various tiers of technology stacks e.g., network, application servers, database servers, etc. k) Secure the development process by integrating security in the CI pipeline (SAST, DAST, SCA, Container Security) while managing vulnerabilities throughout the stack. l) Provide hands-on security training QA and Development teams on security focused unit tests

Minimum Qualification:

a) Bachelor's Degree in computer science, Computer Engineering or related field and/or ten (10) years equivalent work experience.
b) Specialization in IT Security, Forensics, IT Management
c) Certification in one or more of the following: CISSP (Certified Information Systems Security Professional); CEH (Certified Ethical Hacker); CCSE (Check Point Certified Expert); CCSP (Certified Cloud Security Professional); Azure Security Engineer Associate; Microsoft 365 Security Administrator Associate; GWEB (GIAC Web Application Defender); CSSLP (Certified Secure Software Lifecycle Professional)

Role #45 – SOC Analyst

Responsibilities:

a) Providing response and actions needed for security events including but not limited to intrusion detection, malware infections, denial of service attacks, privileged account misuse and network intrusions.
b) Following defined workflow and processes for threat remediation and escalation/handoff where required.
c) Utilizing a variety of cloud-based and on-premises security tools and techniques to proactively analyze suspicious events, network anomalies and other potential threats to determine validity, impact, scope and recovery options.
d) Using automated malware analysis tools to determine threat impact and taking actions appropriately.
e) Support and administration of security tools and platforms in diverse, cloud-based and on-premises environments.
f) Configuring and monitoring Security Information and Event Management (SIEM) platform for security alerts. Integrate and work with the firm's Managed Security Services Provider (MSSP) services staff to guide and manage decisions related to alerts.
g) Improving the service level for security operations and monitoring. Creating and maintaining system documentation for security event processing. Expanding the usage of security monitoring tools to improve the security of the environment based on business use cases or changes in threat landscape, root causes from security incident response, or output from security analytics.
h) Perform duties related to installing MFA (Multi Factor Authentication) on users' machines and helping users with general onboarding.
i) Perform software installation as needed on user machines for security related software
j) Guide new employees and contractor onboarding process by working with individuals to setup access and follow prescribed procedures.
k) Help develop run books and document technical security procedures

Minimum Qualification:

a) Four (4) or more years of relevant work experience.
b) Bachelor's degree in Computer Science, Computer/Data Systems Management or a related field or discipline, and/or equivalent experience
c) Experience in an Operations Center (SOC/NOC) / monitoring environment.
d) Experience working with SIEM technologies (e.g., ArcSight, QRadar, Splunk, Azure Sentinel, etc.) or Managed Security Service Providers (MSSP).
e) GIAC Security Certification such as GSEC, GMON, GISP, or ISC2 CISSP OSCP, GIAC GISP, or GIAC GCIH are preferred.

Role #46 – SOC Lead/Manager

Responsibilities:

a) Manage the SIEM operations and develop processes, procedures and run books.
b) Triage, assess and manage alerts and incidents
c) Manage security incident handling and response operations from end to end, especially L3 and L4 or critical and high incidents in collaboration and through direction from Manager, Cyber Security Operations.
d) Manage the Service tickets (Change, Incidents, Service requests, and problem tickets) and assign based on volume and workload to team members.

e) Develop use cases in MS Sentinel through continuous development and improvements
f) Review and evaluate daily threat feeds
g) Manage vulnerability scanning, analysis and dissemination of vulnerabilities and remediation to SMEs to address identified risks.
h) Manage threat feeds and threat briefings coming from multiple sources to ensure vigilance especially related to critical and high issues uncovered in the technology space.
i) Perform a hands-on investigation as required on systems, applications, networks, Cloud environments etc.,
j) Assist to protect IT hardware, software and data against modification, destruction, and accidental or unauthorized disclosure.
k) Assist in authentication and access control by designing, administering and controlling proven security systems.
l) Analyze IT system vulnerabilities and implement protective measures to back up, restore and secure systems.
m) Lead development projects and complex, highly innovative strategic initiatives, such as the development of IT security standards and policies.
n) Recommend planning and execution of operationally and conceptually complex projects and initiatives that require comprehensive analysis and understanding of the organization and line of business.
o) Coordinate and interact with stakeholders.
p) Subject matter expert, as well as resource person and coach for decision-making bodies.
q) Assist with managing encryption processes such as PGP key management and creation, GOC My key, Entrust SSL certificate management, etc.
r) Lead vulnerability management by conducting scans and completing analysis and communication with SMEs on resolutions and vulnerability tracking.
s) Other security operations duties as assigned

Minimum Qualification:

a) Bachelor's degree
b) A minimum of six (6) years of relevant experience
c) Certifications in one or more of security certifications. GIAC GMON, GIAC GCIH or Other Incident handling and Response, CISSP, CISA, CEH, OSCP, or any other technical certification is an asset.

Role #47 – Cloud Security Specialist

Responsibilities:

a) Develop security strategy plans and roadmaps based on sound enterprise architecture practices
b) Develop and maintain security architecture artifacts (e.g., models, templates, standards and procedures) that can be used to leverage security capabilities in projects and operations
c) Determine baseline security configuration standards for operating systems, network segmentation and identity and access management (IAM)
d) Develop standards and practices for data encryption and tokenization in the organization, based on the organization's data classification criteria
e) Draft security procedures and standards to be reviewed and approved by executive management
f) Track developments and changes in the digital business and threat environments to ensure that they're adequately addressed in security strategy plans and architecture artifacts
g) Validate IT infrastructure and other reference architectures for security best practices and recommend changes to enhance security and reduce risks, where applicable
h) Validate security configurations and access to security infrastructure and application tools, including firewalls, IPSs, WAFs, Keyvaults, Vulnerability Scanners, SIEMs and anti-malware/endpoint protection systems
i) Conduct or facilitate threat modeling of services and applications that tie to the risk and data associated with the service or application
j) Ensure a complete, accurate and valid inventory of all systems, infrastructure and applications that should be logged by the security information and event management (SIEM) or log management tool
k) Coordinate with relevant teams to advocate secure coding practices

l) Coordinate with the privacy officer or office to document data flows of sensitive information in the organization (e.g., PII) and recommend controls to ensure that this data is adequately secured (e.g., encryption and tokenization)
m) Review network segmentation to ensure least privilege for network access
n) Participate in application and infrastructure projects to provide security-planning advice
o) Liaise with the internal audit (IA) team to review and evaluate the design and operational effectiveness of security-related controls
p) Responsible for End-to-End security maintenance and security testing of cloud infrastructure
q) Recommend and implement new services to enhance the security of CDIC's cloud environment based on best practices and guidance from the GOC standards

Minimum Qualification:

a) Bachelor's or Master's degree in computer science, information systems, cybersecurity or a related field and/or ten (10 years equivalent work experience
b) Certification in one or more of the following: CISSP; CCSP; Azure Security Engineer Associate; Microsoft 365 Certified: Security Engineer Associate

Role #48 – Security Administrator

Responsibilities:

a) Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices.
b) Design and implement disaster recovery plan for operating systems, databases, networks, servers, and software applications.
c) Assess need for any security reconfigurations (minor or significant) and execute them if required.
d) Keep current with emerging security alerts and issues.
e) Conduct research on emerging products, services, protocols, and standards in support of security enhancement and development efforts.
f) Recommend, schedule, and perform security improvements, upgrades, and/or purchases.
g) Deploy, manage, and maintain all security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.
h) Administer and maintain end user accounts, permissions, and access rights.
i) Manage Onboarding and Offboarding activities for staff and consultants.
j) Manage connection security for local area networks, the company web site, the intranet, and e-mail communications.
k) Manage and ensure the security of databases and data transferred both internally and externally.
l) Design, perform, and/or oversee penetration testing of all systems to identify system vulnerabilities.
m) Design, implement, and report on security system and end user activity audits.
n) Monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interpret activity and make recommendations for resolution.
o) Recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach.
p) Download and test new security software and/or technologies.
q) Perform system backups
r) Manage and/or provide guidance to junior members of the team.
s) Process Service requests and respond to incidents.

Minimum Qualification:

a) College diploma or university degree in the field of computer science and/or [7] years equivalent work experience.
b) Certification in one or more of the following: CCSA (Check Point Certified Security Administrator); Microsoft 365 Certified: Security Administrator Associate; other Azure and cloud security certifications will be considered also.

Role #49 – Governance Risk and Compliance (GRC) Analyst
Responsibilities:
a) Help define and lead the implementation of an enterprise-wide strategy focused on the reduction of technology risk b) Develop and maintain a Cyber Risk register including critical assets, vulnerabilities and threats. c) Perform threat modeling exercises on a regular and ad-hoc basis to identify existing and new emerging threats relevant to CDIC. d) Develop and maintain Cyber policies, standards, processes, and procedures e) Develop cyber communication plans and content on security awareness and best practices f) Work with IT, business and internal and external audit teams to perform security and compliance assessments on new and existing systems, processes, and technologies g) Participate in disaster recovery and business continuity planning and testing h) Lead efforts to achieve compliance with various frameworks and regulations by consulting and working with the relevant IT and business staff and control owners i) Perform periodic gap assessments to validate compliance on an ongoing basis to ensure that proper controls are in place and risks are appropriately mitigated.
Minimum Qualification:
a) Bachelor's degree in Information Systems, Cybersecurity, or a related field and/or five (5) years equivalent work experience. b) Three (3+) years of relevant experience in the IT risk, security, compliance or audit field c) Certification in one or more of the following: CISSP (Certified Information Systems Security Professional); CRISC (Certified in Risk and Information Systems Control)

D. Description for Roles in the Initial RFSA

1. <u>The following are the specific descriptions for each Role in Service Category #1 - Advisory Services:</u>

Role #1 - IT Executive Strategic Advisor
Responsibilities:
a) Provide vision and leadership in delivering on the strategic goals of CDIC by establishing the IT department's vision and mission and leading the implementation of the IT Strategic Plan; b) Develop an intimate understanding of CDIC's strategy and services to provide expertise on how to build and deploy scalable technology during expansion in the core and new business models; c) Ensure that architecture, governance and assurance exist, remove inefficiency in processes and champion standards that support business objectives and enable IT transformation; d) Ensure the security of the business, its staff and customers, as well as IT assets; e) Advise Senior Management on strategic system conversions and integrations in support of business goals and objectives; f) Be at the forefront of technology, assessing new computing technologies to determine potential value for the corporation; g) Manage and continuously adapt the future-state enterprise architecture; h) Manage the IT budget and develop IT capital investment plans for implementing IT initiatives from the IT Roadmap and Strategic Plan; i) Ensure that leading practices for IT governance, security, operations, development, projects and risk management are leveraged and practiced within IT and across the broader organization; j) Manage relationships with strategic IT partners and vendors; and k) Establish relevant and appropriate metrics and monitor and continuously improve service delivery performance.
Minimum Qualification:
a) University degree in Business, IT or a related discipline b) Experience in business and strategic advisory within IT

Role #2 - Data Strategy Advisor
Responsibilities:
a) Develop and deliver long-term strategic goals for data architecture vision and standards in conjunction with data users, department managers, clients, and other key stakeholders; b) Participate in the creation and ongoing operation of the corporate data strategy and establish policies and procedures for sound data governance; c) Conceptualize data products including dashboards and visualizations required to meet the organization's objectives; d) Create short-term tactical solutions to achieve long-term objectives and an overall data management roadmap; e) Establish processes for governing the identification, collection, and use of corporate metadata; take steps to assure metadata accuracy and validity; f) Establish methods and procedures for tracking data quality, completeness, redundancy, and improvement; g) Conduct data capacity planning, life cycle, duration, usage requirements, feasibility studies, and other tasks; h) Create strategies and plans for data security, backup, disaster recovery, business continuity, and archiving; i) Ensure that data strategies and architectures are in regulatory compliance; and j) Assess and cultivate long-term strategic goals for database development in conjunction with end users, managers, clients, and other stakeholders.
Minimum Qualification:
a) University degree in a related field b) Certification related to business intelligence c) Experience as a Business Intelligence / Data Warehouse (BI/DW) Specialist

2. <u>The following are the specific descriptions for each Role in Service Category #2 - Project Management:</u>

Role #3 - Project Management Office Lead
Responsibilities:
a) Establish, implement, develop, and control best practices for IT project management throughout the organization; b) Lead complex transformation programs and ensure each project stream/component is managed using appropriate processes, tools and disciplines; c) Build, maintain and oversee the enterprise program management framework using 'agile' practices for driving program deliverables; d) Oversee and maintain the overall program delivery schedule, integrating with individual work-stream schedules and clearly showing timeframes, resourcing, dependencies and critical paths; e) Support subordinate CDIC Program Project Managers in overseeing the provision of all resources for the project (internal, vendor, other contractors, any other third party/seconded resources); f) Support subordinate CDIC Program Project Managers in reviewing and maintaining all statements of work for all project activities; manage and report on all program financials, including forecasts, reporting actuals and explaining variances to budgets; g) Support CDIC in preparing for and managing change associated with Modernization including change readiness assessment; collaboration with CDIC's Enterprise Risk Management (ERM) team; provide content to the Communications representatives; h) Coordinate the governance process for transformation programs, preparing reporting for governing bodies; and i) Develop and manage a program to periodically assess the quality of work and satisfaction with vendor and wider team performance, identifying issues and remedial actions, and coordinating actions to address issues.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) PMP certification c) Experience as an IT Project Manager

Role #4 - Project Manager
Responsibilities:
a) Manage the project during the development, implementation and operations start-up by ensuring that resources are made available and that the project is developed and is fully operational within previously agreed time, cost and performance parameters; b) Formulate statements of problems; establish procedures for the development and implementation of significant, new or modified project elements to solve these problems, and obtains approval thereof; c) Define and document the objectives for the project; determine budgetary requirements, the composition, roles and responsibilities and terms of reference for the project team; d) Report progress of the project on an ongoing basis and at scheduled points in the life cycle; e) Meet in conference with stakeholders and other project managers and state problems in a form capable of being solved; f) Prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools; g) Manage several Project Managers, each responsible for an element of the project and its associated project team; and h) Support development of project management procedures, tools and forms.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) PMP certification c) Experience as an IT Project Manager

Role #5 - Project Administrator / Coordinator
Responsibilities:
a) Assist project management and data processing professionals, technical users and end users in project coordination and synchronization tasks; b) Provide administrative and technical support of a clerical nature as required to a project team; c) Assist in performing such tasks as maintaining project documentation and application/system libraries; d) Act as the first or single point of contact in a "hot-line" situation by accepting incoming calls, logging calls, attempting to resolve simple problems and following established procedures for more difficult problems; e) Track project change requests; f) Maintain and update relevant project information in manual and/or electronic files; project information might include such things as project activity schedule, status reports, correspondence; g) Use computer tools, aids, system control languages on Personal Computers (PCs), minis, or mainframes to perform work; h) Communicate with project management and data processing professionals, technical users and end users on administrative matters related to the project; and i) Assist in the development of standardized project and communications tools.
Minimum Qualification:
a) Post-secondary diploma/degree in a related field

3. <u>The following are the specific descriptions for each Role in Service Category #3 - Cyber Security:</u>

Role #6 - Security Analyst
Responsibilities:
a) Primary duty is the day-to-day operations of the in-place security solutions and the identification, investigation and resolution of security breaches detected/reported by the business; b) Participate in the planning and design of enterprise security architecture, under the direction of the IT Security Manager, where appropriate; c) Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures) under the direction of the IT Security Manager, where appropriate;

d) Participate in the planning and design of an enterprise Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), under the direction of the IT Security Manager, where appropriate;
e) Review logs and reports of all in-place devices, whether they be under direct control (i.e. security tools) or not (e.g. workstations, servers, network devices); interpret implications of that activity and devise plans for appropriate resolution;
f) Participate in investigations into problematic activity;
g) Participates in disaster recovery testing;
h) Develops and implements business and IT continuity/recovery strategies;
i) Provides advice and guidance to technical teams in the performance of their duties related to the ongoing design, development and implementation of continuity/security recovery capabilities in the areas of infrastructure (hardware, software, and networks), application development, and data management;
j) Develops Risk Management deliverables including Threat Risk Assessments (TRA), Statements of Sensitivity (SOS), Vulnerability Analysis (VA) and/or Security Gap Analysis evaluating Information Technology Safeguards (ITS) safeguards;
k) Defines Recovery Objectives and Timeframes, including recovery times, expected losses, and priorities;
l) Researches and documents solutions for Intrusion Detection, Secure Networks, User Management and Control Systems, Information Protection Strategies, Recovery Requirements, and Information Technology Security Evaluation Criteria (ITSEC) challenges;
m) Prepares Cost/Benefit Analysis of ITSEC and Recovery Strategies and presents findings to Senior Management;
n) Conducting Threat Risk Assessments using qualitative and quantitative risk analysis methodologies such as annual loss expectancy, estimated annual cost, threat tree analysis, cause-sequence analysis, hazard and operability analysis, interface analysis and consultative, objective and bi-functional risk analysis;
o) Configure and manage enterprise firewalls, including the modification firewall rules, analyzing firewall log files and implementing corrective action;
p) Participate in the design and execution of vulnerability assessments, penetration tests, and security audits;
q) Perform the deployment, integration, and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically and CDIC's security documents specifically; and
r) Recommend additional security solutions or enhancements to existing security solutions to improve overall enterprise security.

Minimum Qualification:

a) University degree in a related field
b) Certified Information Systems Security Professional (CISSP)

Role #7 - Application Security Administrator

Responsibilities:

a) Development, configuration, testing, deployment and integration of application security;
b) Design, perform, and/or oversee penetration testing of all applications to identify system vulnerabilities;
c) Perform security reviews of applications through code implementation and review, application configuration and penetration testing;
d) Encryption of Transport Layer Security (TLS) in transit and database encryption at rest;
e) Design, implement, and report on security system and end user activity audits;
f) Design and implement Disaster Recovery Plan for operating systems, databases, networks, servers, and software applications;
g) Deploy, manage, and maintain all security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and antivirus software;
h) Monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity; interpret activity and make recommendations for resolution;
i) Recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach;
j) Assess need for any security reconfigurations (minor or significant) and execute them if required;

k) Interact and negotiate with vendors, outsourcers, and contractors to obtain protection services and products;
l) Recommend, schedule, and perform security improvements, upgrades, and/or purchases;
m) Manage and/or provide guidance to junior members of the team; and
n) Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices.

Minimum Qualification:

a) University degree in a related field
b) Previous experience as a Security Analyst
c) Knowledge of Open Web Application Security Project (OWASP), Secure Sockets Layer / Transport Layer Security (SSL/TLS) and Transmission Control Protocol / Internet Protocol (TCP/IP) protocols

Role #8 - IT Security Architect

Responsibilities:

a) Designing and developing security architecture patterns that meet regulatory obligations and data protection requirements as well as align the business and corporate security strategy;
b) Perform security assessments, identify gaps in existing security architecture, and recommend changes or improvements;
c) Assist in developing Disaster Recovery and Business Continuity Plan; identify and prioritize system functions required to promote continuity availability of critical business processes;
d) Direct equipment and software installation and prepare preventative and reactive measures;
e) Research information security standards, conduct systems security and vulnerability analyses and risk assessments; identify integration issues; prepare effort estimates;
f) Define and document how the implementation of a new technology impacts the security posture of the current environment;
g) Determine security requirements by evaluating business strategies and requirements;
h) Define security strategies for CDIC by specifying intrusion detection methodologies and equipment;
i) Enhance security team accomplishments and competence by planning delivery of solutions, answering technical and procedural questions, teaching improved processes to other Security Architects; and
j) Provide input on security requirements to be included in requests for proposal (RFPs), statements of work (SOWs), and other procurement documents.

Minimum Qualification:

a) BSc. in Cyber Security, Information Systems, Information Technology, or Computer Science
b) Appropriate Security Certifications, CISSP, Certified Information Security Manager (CISM), Global Information Security Professional (GISP), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Auditor (CISA)
c) Certifications in Certified Information Systems Security Professional – Information Systems Security Architecture Professional (CISSP-ISSAP), The Open Group Architecture Framework (TOGAF), or Sherwood Applied Business Security Architecture (SABSA)
d) Previous relevant experience in IT security architecture
e) Azure/O365 Cloud experience is an asset

Role #9 - Ethical / White Hat Hacker (or Penetration Tester)

Responsibilities:

a) Primary duty includes conducting security assessment on networks as well as on application level;
b) Perform network penetration, web application testing, source code reviews and threat analysis;
c) Develop comprehensive and accurate reports and presentations for both technical and executive audiences;
d) Model and/or Handle threats for applications, systems, infrastructure and concepts;
e) Plan coordinate and simulate attacks;
f) Analyze components and configurations in finding out weak points;
g) Develop proposals for an appropriate counteraction and generate analysis and reports;
h) Provide recommendations to remediate identified gaps;

i) Present results to different committees; and j) Conduct workshops or live hackings at the customers location or in-house.
Minimum Qualification:
a) BSc. in Cyber Security, Information Systems, Information Technology, or Computer Science or related field b) Certified Ethical Hacker, SysAdmin, Audit, Network and Security Global Information Assurance Certification (SANS GIAC), Penetration Testing, Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE) c) Azure/O365 Cloud experience is an asset d) Relevant experience as a Penetration Tester and/or IT Security Analyst, Developer/Software Engineer, Network Administrator or Security Engineer

Role #10 - Azure Security Architect
Responsibilities:
a) Provides subject matter expertise and supports the design, deployment, configuration and monitoring/evaluation of secure Cloud infrastructure; supports the conduct of security assessments and risk analysis, providing risk avoidance, mitigation and issue resolution.
Minimum Qualification:
a) Degree/diploma in Computer Science, Computer Engineering, Information Technology or equivalent b) Microsoft Certified: Azure Security Engineer Associate or equivalent Microsoft Certification c) Experience defining and configuring secure IT networks and system architectures in MS Azure, including virtual machines, virtual networks and endpoints d) Experience implementing Azure Network Security Appliances and using Azure Security Centre e) Experience applying Information Technology Security Guidance (ITSG-33) and government security standards in a Cloud environment f) Previous experience in the role

NOTE TO SUPPLIERS: It is anticipated that the technologies for Service Category #11 - Business Intelligence and Analytics will be mainly the Microsoft BI stack, including Azure, as well as Tableau and Alteryx.

Role #11 - Azure Security Administrator
Responsibilities:
a) Supports the design/definition of, and configures and manages, network and system encryption and system security and access controls.
Minimum Qualification:
a) Microsoft Certified: Azure Security Engineer Associate or equivalent Microsoft Certification b) Experience applying ITSG-33 and government security standards in a Cloud environment c) Experience implementing Azure Network Security Appliances and using Azure Security Centre

4. <u>The following are the specific descriptions for each Role in Service Category #4 - Enterprise Technology:</u>

Role #12 - Storage Administrator / Virtualization Architect
Responsibilities:
a) Operation and performance tuning of storage platforms across CDIC to ensure high levels of data quality, availability and security; b) Perform tasks necessary to fulfill Service Level Agreements (SLA's) with end-users regarding storage allocations, limitations, security and availability; c) Perform/test backups and restores to ensure that enterprise data is effectively protected; d) Anticipate, mitigate, identify, respond to, and resolve issues with storage devices, storage access, and data retrieval; e) Research and make recommendations on storage products, services, and standards in support of procurement/development efforts;

f) Monitor, analyze, and predict trends for storage equipment performance, space allocation, and data growth to recommend enhancements to the IT storage team;
g) Develop routines for end-users to facilitate storage best practices, including desktop storage administration;
h) Perform storage server/database transaction and security audits leading to identification and mitigation of security threats to enterprise data; recommend and implement changes where necessary;
i) Work with systems and Database Administrators to implement storage architectures that utilize best practices;
j) Implement redundant systems, policies, and procedures for disaster recovery and archiving to ensure effective protection and integrity of storage appliances and stored data assets;
k) Participate in and support capacity planning and development of long-term strategic goals for CDIC's storage in conjunction with data owners and department managers; and
l) Participate in the planning and implementation of policies and procedures to ensure storage provisioning, efficiency and maintenance that is consistent with CDIC's goals, industry best practices and regulatory requirements.

Minimum Qualification:

a) BSc. in Cyber Security, Information Systems, Information Technology, Computer Science or related field and/or related technical diploma
b) Previous relevant experience in Storage Architecture

Role #13 - Systems Architect (Network, Data, Applications)

Responsibilities:

a) Develop technical architectures, frameworks and strategies, either for an organization or for a major application area, to meet the business and application requirements;
b) Analyze and evaluate alternative technology solutions to meet business problems;
c) Ensures the integration of all aspects of technology solutions;
d) Analyze functional requirements to identify information, procedures and decision flows;
e) Evaluate existing procedures and methods; identify and document database content, structure, and application sub-systems, and develop data dictionary;
f) Define and document interfaces of manual to automated operations within application sub-systems, to external systems and between new and existing systems;
g) Define input/output sources, including detailed plan for technical design phase, and obtain approval of the system proposal;
h) Model business and systems processes based on findings through use case scenarios, workflow diagrams, and data models;
i) Develop and execute test plans to check infrastructure and systems technical performance; report on findings and make recommendations for improvement;
j) Develop and manage a systems capacity plan;
k) Provide guidance to junior members of the team;
l) Identify the policies and requirements that drive out a particular solution;
m) Monitor industry trends to ensure that solutions fit with government and industry directions for technology;
n) Identify and document system specific standards relating to programming, documentation and testing, covering program libraries, data dictionaries, naming conventions, etc.;
o) Design and implement long-term strategic goals and short-term tactical plans for managing and maintaining corporate systems and software;
p) Ensure that proposed and existing systems architectures are aligned with organizational goals and objectives;
q) Provide architectural expertise, direction, and assistance to Systems Analysts, Systems Engineers, other Systems Architects, and software development teams; and
r) Review new and existing systems design projects and procurement or outsourcing plans for compliance with standards and architectural plans.

Minimum Qualification:

a) University degree in a related field
b) Previous relevant experience as a Systems Architect

Role #14 – Azure Architect
Responsibilities:
a) Provides subject matter expertise in Cloud Architecture and supports the design, deployment, configuration and monitoring/evaluation of Azure infrastructure, networking, applications, data platform and solution administration; conducts analysis and provides expert support to the planning and conduct of migration projects.
Minimum Qualification:
a) Degree/diploma in Computer Science, Computer Engineering, Information Technology or equivalent b) Microsoft Certified: Azure Solutions Architect or equivalent Microsoft Certification

Role #15 - Azure Administrator
Responsibilities:
a) Supports system design and implementation, including install/creation, configuration, deployment, monitoring/maintenance and evaluation, focusing on compute, storage, networking, security, and integration aspects, including user administration.
Minimum Qualification:
a) Microsoft Certified Azure Administrator Associate or equivalent Microsoft Certification b) Previous relevant experience in the role

Role #16 - Azure Data Base Administrator
Responsibilities:
a) Supports the design and implementation of database solutions for Structured Query Language (SQL) Server and MS Azure, including database security, availability, performance, scalability and recovery requirements.
Minimum Qualification:
a) Degree/diploma in Computer Science, Computer Engineering, Information Technology or equivalent b) Microsoft Certified Solutions Associate (MCSA) SQL 2016 (any), Microsoft Certified Technology Specialist, Microsoft Certified IT Professional, or equivalent Microsoft Certification c) Hands on technical experience with SQL Server

Role #17 - Webmaster
Responsibilities:
a) Coordination, planning, maintenance and accessibility of web site content while ensuring the consistency of the web site's look and feel; b) Create web pages including graphics and general web site design; c) Find, diagnose, and fix web site problems, including broken links (both internal and external), typographical errors, and formatting inconsistencies; d) Develop and implement usability tests, analyze results and modify design accordingly; e) Develop flowcharts (web site flow maps) depicting navigation and basic content; f) Develop line drawings or block diagrams illustrating the priority of information, links, navigation, and space requirements; g) Develop content diagrams showing the interactive connection between web pages; h) Develop interactive prototypes showing basic form and functionality for both usability testing and presentations; i) Prepare a long-term plan for web site development and presence, including standards and guidelines for content, based on business goals and input from stakeholders; and j) Manage the acquisition and ongoing maintenance of the organization's domain names with the appropriate registrars.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Previous relevant experience as a Webmaster

5. <u>The following are the specific descriptions for each Role in Service Category #5 - Technical Support:</u>

Role #18 - Application Support Specialist
Responsibilities:
a) Installation, maintenance and troubleshooting of desktop computers, laptops and printer hardware and associated software as well as providing remote support for external desktop computer and laptop connections, wireless, and broadband; b) Providing problem recognition, isolation, research, resolution and follow-up; c) Providing 2nd level technical support; d) Providing systems administration duties such as creating and maintaining network accounts, performing basic security back-ups; e) Escalating more complex problems to senior support personnel to expedite resolution; f) Assisting with the automation of desktop computer build processes and packaging applications; g) Troubleshooting and resolving network problems; h) Creating problem and resolution logs for help desk activities; i) Ensuring technical support issues are resolved in a prompt and efficient manner; j) Conducting basic development support services such as patch development and other related application support services; k) Planning or participating in the implementation of organization wide system upgrades, occasional project work, asset management, technical documentation and making recommendations on technology; l) Creating and deploying feedback mechanisms for end users; analyzing results, making recommendations for support process improvements, and implementing changes; m) Resolving advanced application support issues; n) Coordinating emerging technology application specifications; o) Conducting research into software application products and services in support of development and purchasing efforts; p) Solving complex end-user technical problems that more junior levels cannot resolve; q) Serving as a user support liaison between vendors, information systems technicians, and end-user organizations; r) Providing training expertise and direction in the area of emerging technology and special application support; s) Emulating or reproducing technical problems encountered by users; t) Providing advice and training to users in response to identified difficulties; u) Recommending and implementing complex security requirements; v) Providing business systems, network and Internet support to users in response to identified difficulties; and w) Collecting, organizing and maintaining a problems and solutions log for use by others.
Minimum Qualification:
a) Certificate, diploma, or degree in Computer Science or other relevant field from a recognized post-secondary institution is required b) Previous relevant experience as an Application Support Specialist

Role #19 - Deskside Technical Support Analyst
Responsibilities:
a) Provide basic technical support / assistance to organization personnel for its standard desktop software suite, as well as printers and other peripherals; and b) Provide support for mobile devices, including related apps / software and peripherals.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Previous relevant experience as a Technical Support Analyst

Role #20 - Service Desk Analyst
Responsibilities:
a) Perform a variety of network problem analysis and monitoring tasks, monitor network management systems and respond appropriately to user requests and problems; b) Perform initial problem analysis and triage problems to other appropriate staff when appropriate; c) Maintain liaison with network users and technical staff to communicate the status of problem resolution to network users; log and track requests for assistance; d) Participate in on-site installations of network systems for users; e) Perform other related duties incidental to the work described herein; and f) Develop, implement, and/or participate in the distribution of network related information to users to include information such as help desk procedures and network handbooks.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Previous relevant experience as a Service Desk Analyst

Role #21 - IT Service Management Specialist
Responsibilities:
a) Create and implement processes and procedures following Information Technology Service Management (ITSM) Best Practices; b) Review and evaluate existing processes and procedures following ITSM Best Practices; c) Provide guidance to CDIC staff in applying ITSM Best Practices; d) Provide knowledge transfer to CDIC employees; e) Develop, implement, and/or participate in the preparation of procedure manuals and documentation for help desk use; f) Conduct periodic user satisfaction surveys and track user problem trends; make recommendations for improvements to the network systems and create reports based on information provided from user surveys and trends; g) Record, monitor and report on service desk performance; and h) Participate in the development of a comprehensive training plan for help desk procedures; assist in training personnel providing backup coverage.
Minimum Qualification:
a) University degree in a related field b) Previous relevant experience as an ITSM Specialist, consulting on, developing, implementing and applying IT Service Management principles and processing

Role #22 - Security Incident Responder
Responsibilities:
a) Duties include responding to security incidents as they arise and manage incidents end-to-end; b) Use appropriate logs and tools to determine whether breach has occurred and document scope of event(s); c) Determine risks to CDIC by evaluating risk using standard metrics; d) Escalate incidents according to protocol and ensure all necessary parties are informed and actively engaged; e) Conduct incident and investigation post-mortem briefings, analysis and reporting to determine the background, current state; identify the root cause or error and identify escalation team; f) Collect and preserve evidence to be admissible in court if needed; g) Develop and design approaches necessary to respond to incidents; h) Build scripts, tools, or methodologies to enhance CDIC's incident investigation processes; i) Produce detailed incident reports and technical briefings for technical, administrator and end-users; and j) Liaison with security entities.
Minimum Qualification:
a) BSc. in Cyber Security, Information Systems, Information Technology, or Computer Science b) Relevant certifications e.g. Certified Incident Analyst (GCIA), Certified Computer Security Incident Handler (CSIH), Network Forensic Analyst (GNFA), Forensic Analyst (GCFA), Council for

Registered Ethical Security Testers (CREST) Certified Incident Manager, or CREST Certified Network Intrusion Analyst
c) Previous relevant incident response and cyber experience
d) Azure/O365 Cloud experience is an asset

Role #23 - Infrastructure Operations and Support

Responsibilities:

a) Test network performance and provide network performance statistics and reports; develop strategies for maintaining network infrastructure;
b) Consolidation of parallel networks onto a shared public or private infrastructure and integrating networks of recently merged or acquired enterprises into the original enterprise's network system;
c) Provides technical planning and support for a medium complexity network in a single location with some Virtual Private Network (VPN) connectivity;
d) Provides technical planning and support for high-end core Local Area Network (LAN) Switching products, including layer-3 switching;
e) Supports a production TCP/IP wide-area network;
f) Provides Open Shortest Path First (OSPF), point-to-point and multipoint designs;
g) Develops and maintains Network system documentation;
h) Performs network troubleshooting;
i) Reviews coding and error detection methodologies;
j) Collect and preserve evidence to be admissible in court if needed;
k) Supporting the development of business cases;
l) Provides input into network modeling and simulation exercises;
m) Interprets the needs of applications and users into logical designs, SLAs and network management practices;
n) Writes technical specifications, acceptance criteria, and performs evaluation of technical proposals for network related RFPs in a public sector environment;
o) Assesses the impact of new applications and application changes in the Network;
p) Leads technical teams in specific Network improvement and upgrade projects.
q) Provides TCP/IP Network Management;
r) Reviews communications over local and wide area networks as to their ability to support data processing requirements;
s) Recommends changes to transmission networks, both in terms of hardware devices and switching points required to improve network performance;
t) Participates in the analysis, design, and implementation of communication networks for data processing transmissions requirements;
u) Support and manage storage, including Storage Area Network (SAN) and Network-Attached Storage (NAS) types;
v) Design and recommend short and long-term strategic plans to ensure infrastructure capacity meets existing and future requirements;
w) Reviews cabling standards and building designs;
x) Provides networking solutions to all server platforms;
y) Researches, tests and recommends the adoption of new technologies, hardware, and software and network protocols to enhance data processing requirements;
z) Recommends and coordinates the removal of outdated technologies, software and network protocols while maintaining or enhancing existing data processing requirements;
aa) Analyze, make recommendations for, and implement various virtualization projects / initiatives;
bb) responsible for providing technical support for on premises and Cloud (Azure and O365) technology; and
cc) support operations for disaster recovery to ensure the effective backup and recovery of CDIC data.

Minimum Qualification:

a) Post-secondary degree/diploma in a related field such as Computer Technology, Networking, Computer Science, or related field
b) Previous relevant experience as an Infrastructure Operations and Support Specialist

Role #24 - Technical Writer / Trainer / Courseware Author (developer)
Responsibilities:
a) Document help text, user manuals, technical documentation, web page content, etc.; b) Gather information concerning the features and functions provided by Developers; c) Develop a table of contents for each document/manual and write or edit the required content; d) Investigate the accuracy of the information collected by making direct use of the material being documented; e) Prepare or coordinate the preparation of any required illustrations and diagrams; f) Design the layout of documents / manuals; g) Use word-processing, desktop publishing and graphics software packages to produce final camera-ready copy; h) Review documentation standards and the existing project documentation; i) Determine documentation requirements and make plans for meeting them; j) Assess the audience for the documents/manuals which are required and prepare a statement of purpose and scope for each; k) Perform needs assessment/analysis for training purposes; l) Plan and monitor training projects; m) Perform job, task, and/or content analysis; n) Write criterion-referenced, performance-based objectives; o) Recommend instructional media and strategies; p) Develop performance measurement standards; q) Develop training materials; r) Prepare end-users for implementation of courseware materials; s) Communicate effectively by visual, oral, and written form with individuals, small group, and in front of large audiences; and t) Develop and deliver IT-related training material to small and medium-sized groups (5 to 50).
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Previous relevant experience as a Technical Writer

6. <u>The following are the specific descriptions for each Role in Service Category #6 - SharePoint Support:</u>

Role #25 - SharePoint Online Administrator
Responsibilities:
a) Administration of collaboration tools in support of CDIC's SharePoint tenants; b) Oversee activity pertaining to the maintenance of SharePoint including incident and request tickets; c) Responsible for maintaining end user access permissions and related system guidelines; d) Provide defect and issue resolution to end users; e) Establishing access and control guidelines, maintain and monitor related infrastructure and develop standards for use of systems; f) Recommend, schedule, and perform software and hardware improvements, upgrades, patches, reconfigurations, and/or purchases; g) Coordinates with product vendors and/or service providers to resolve technical issues; and h) Participate in and support capacity planning and the development of long-term strategic goals for SharePoint in conjunction with end-users and department managers.
Minimum Qualification:
a) Degree/diploma in Computer Science, Computer Engineering, Information Technology or equivalent b) Previous relevant experience in the role

Role #26 - SharePoint Online Architect
Responsibilities:
a) Leading the SharePoint team in the analysis, design development and deployment of SharePoint solutions; b) Primary architect for all custom SharePoint solutions; lead complete software development life cycle, including design, analysis, configuring, programming and testing;

c) Educate developers on best practices for developing custom SharePoint solutions;
d) Provide expertise and support to business managers and other members of IT to determine how to best implement, support, and use SharePoint solutions;
e) Participate in SharePoint infrastructure projects;
f) Determine when SharePoint is not the right solution for a business problem and communicate this effectively to business leaders; and
g) Conduct research on emerging SharePoint development tools and strategies.

Minimum Qualification:

a) Degree/diploma in Computer Science, Computer Engineering, Information Technology or equivalent
b) Previous relevant experience with SharePoint Architecture
c) Previous relevant experience in SharePoint development creating solutions (apps, page layouts, workflows etc.)
d) Experience with design, development or enterprise level portals

Role #27 - SharePoint Online Developer

Responsibilities:

a) Design and develop portal content and applications that integrate with other enterprise systems and third-party products;
b) Integrate non-SharePoint related services into SharePoint applications as needed;
c) Assist other Developers, Analysts, and Designers in conceptualizing and developing SharePoint solutions;
d) Provide expertise and support to end users and other members of the IT support team;
e) Conduct research on emerging SharePoint development tools and strategies; and
f) Recommend, schedule, and perform software improvements and upgrades.

Minimum Qualification:

a) College diploma or University degree in the field of Computer Science or Software Engineering, and/or other relevant degree
b) Experience developing web applications using Microsoft and compatible technologies including SharePoint 2007/2010, Visual Studio, VB.Net, and C#
c) Experience in .Net
d) Experience with SharePoint

7. <u>The following are the specific descriptions for each Role in Service Category #7 - Salesforce Support:</u>

Role #28 - Salesforce Developer

Responsibilities:

a) Maintenance and further development of CDIC's Salesforce solution and various apps integrated within the platform;
b) Responsible for the maintenance and development of Salesforce applications;
c) Meet with business teams to determine business, functional and technical requirements and participate in application design, configuration, testing and deployment;
d) Perform configuration and customization of the Salesforce platform;
e) Create related processes, workflow rules and testing;
f) Participate in efforts to develop and execute testing, training and documentation;
g) Assist with the planning of application changes, development, and installation of upgrades and new releases;
h) Provide in depth analysis of production issues and resolve in timely manner;
i) Utilize best practices to perform operational support, enhancements, bug fixes as needed to the Salesforce.com platform;
j) Follow CDIC's standard operating procedures and processes and maintain updated ticketing for events, incidents, requests, changes, problems, etc.;
k) Develop, document and enforce application standards and procedures for Salesforce platform; and

l) Provide technical assistance and end user troubleshooting for bug fixes, enhancements, and "how-to" assistance.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Previous relevant experience as a Salesforce Developer c) Expertise in development and configuration of the Salesforce platform d) Experience in translating business user requirements into well-architected solutions that best leverage the Salesforce platform and products e) Knowledge and experience with the development, testing, and documenting of work on custom development, integrations, and data migration elements of a Salesforce implementation

Role #29 - Salesforce Tester
Responsibilities:
a) Supervision of testing activities in accordance with the plan; b) Management and monitoring of test plans for all levels of testing; c) Management of walkthroughs and reviews related to testing and implementation readiness; d) Development of test plans and coordination; e) Management Status reporting; f) Development of test scenarios and test scripts; g) Conduct of Functional Testing, Unit Testing, Manual Testing, Automated Testing, Load Testing, Deployment Testing, and Security Testing related to Salesforce platform; h) Development and maintenance of testing standards and methodologies; and **i)** Development of QA/testing manuals, procedures, and performance measurement tools.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Previous relevant experience as a Salesforce Tester

Role #30 - Salesforce Administrator
Responsibilities:
a) Support CDIC's ongoing development of Salesforce.com deployment; b) Work closely with functional leaders, business units, and subject matter experts to identify develop and deploy new business processes using the Salesforce platform; c) Serve as primary system administrator for the Salesforce.com environment; d) Handle all basic administrative functions including user account maintenance, reports and dashboards, workflows and other routine tasks; e) Complete regular internal system audits and prepare for upgrades as required; f) Manage Salesforce.com data feeds and other integrations; g) Coordinate the evaluation, scope and completion of new development requests; h) Work with our institutional management team to establish suitable processes to support administrative, development, and change management activities; i) Assist in training of new users, and grow the Salesforce.com skill set across the corporation; j) Effectively act as the liaison between our users, vendors and the application development teams; k) Development of QA/testing manuals, procedures, and performance measurement tools; and l) Support Salesforce system design and implementation, including configuration, deployment, monitoring/maintenance and evaluation, focusing on efficiency of the solution and meeting the needs of business users.
Minimum Qualification:
a) Post-secondary diploma/degree in a related field b) Previous relevant experience as a Salesforce Administrator

8. The following are the specific descriptions for each Role in Service Category #8 - Alteryx Support:

Role #31 - Alteryx Developer
Responsibilities:
a) Develops Alteryx workflows, including macros and analytic applications for high performance processing of high volumes of data.
Minimum Qualification:
a) Education in a field of study related to data analysis (e.g. Information Systems, Computer Science, etc.) b) Previous relevant experience in the field of Business Intelligence and Analytics c) Three (3) years of experience designing and developing/configuring workflows in Alteryx Designer and Alteryx Server d) Experience with SQL e) Experience with architecting high-performance solutions using Relational Databases f) Experience in incremental/iterative (“agile-like”) development and configuration for data solutions g) Expertise in development and configuration using Alteryx Designer and Alteryx Server

9. The following are the specific descriptions for each Role in Service Category #9 - Agile Application Delivery:

Role #32 - Scrum Master
Responsibilities:
a) Serve as liaison between technical and non-technical departments; b) Maintain process documentation; c) Track and communicate team velocity and sprint/release progress; d) Assist as needed with backlog maintenance; e) Assist with prioritization and resolution of defects / bugs; f) Identify and remove impediments, prevents distractions; g) Communicate with other management, developers, product managers and technical support specialists on product issues; h) Organize and facilitate project planning, daily stand-up meetings, reviews, retrospectives, sprint and release planning, demos and other Scrum-related meetings; i) Ensure the development teams are practicing the core agile principles of collaboration, prioritization, team accountability, and visibility; j) Assist with internal and external communication, improving transparency, and radiating information; k) Participate proactively in developing and maintaining team standards, tools, and best practices; l) Facilitate discussion and conflict resolution; and m) Empower the team to self-organize.
Minimum Qualification:
a) Education in a field of study related to software delivery b) Experience leading Scrum meetings and providing team support during sprint planning and execution c) Experience providing coaching to agile teams d) Experience assisting teams with prioritizing and managing of sprint backlog to ensure timely and accurate product delivery e) Experience helping teams deal with any barriers to successful delivery f) Previous relevant experience in similar agile-focused role

Role #33 - Agile Team Coach
Responsibilities:
a) Work closely with Scrum Masters to help team members to develop skills that will lead to the improvement of development processes; share their experience and observations with all team members in order to promote the use of agile best practices; agile team coaches see to the overall objective cohesion of projects involving many teams;

b) Communicate with management, Scrum Masters, Developers, product owners, and technical support specialists about agile best practices;
c) Communicate team progress with Enterprise Agile Coach and Senior Management;
d) Coach Scrum Masters in effective agile delivery;
e) Conflict resolution;
f) Continuous improvement;
g) Cross-functional team development;
h) Removing impediments;
i) Assist with internal and external communication, improving transparency, and radiating information;
j) Aid in the establishment of team metrics to help IT management stay informed about team progress;
k) Participate proactively in developing an Agile Centre of Excellence;
l) Identify knowledge gaps and educate project leadership and development team to close these gaps; and
m) Coach teams to assist them in becoming self-organizing.

Minimum Qualification:

a) Four-year College diploma or University degree in Computer Systems Design or Computer Science, and/or 10+ years equivalent work experience
b) Must possess formal certification as either a Scrum Master or an Agile Coach
c) Previous relevant project management and Scrum Master experience
d) Thorough understanding of agile software development methodologies, values, and procedures
e) Thorough understanding of the software development life cycle
f) Understanding of organization's project management approach
g) Ability to understand technical issues at a high level

10. <u>The following are the specific descriptions for each Role in Service Category #10 - Application Development:</u>

Role #34 - Solution Architect

Responsibilities:

a) Supports the design, deployment, configuration and monitoring/evaluation of infrastructure, networking, applications, data platform and solution administration;
b) Document and develop in-depth knowledge of CDIC's existing architecture;
c) Assist with the design, development and implementation of systems;
d) Manage the schedule of reviews that need to take place for projects that are in progress;
e) Supports the design, deployment, configuration and monitoring/evaluation of infrastructure, networking, applications, data platform and solution administration;
f) Provide guidance to the junior staff in the early planning stage around the different solution patterns that may be appropriate for the specific solution;
g) Inform stakeholders of solution architecture review outcomes;
h) Ensure that the IS, Data, and IT Architecture interests are considered and engagement with the respective architects occurs for all solutions;
i) Ensure that all individual solution architecture artifacts and changes are documented as per process standards and stored in the corporation's IA Library to facilitate compliance, organization, and access;
j) Manage and continuously improve the design and implementation of solution architecture processes and artifacts;
k) Provides subject matter expertise in technical solutions architecture and supports the design, deployment, configuration and monitoring/evaluation of infrastructure, networking, applications, data platform and solution administration; conducts analysis and provides expert support to the planning and conduct of migration projects;
l) Ensure that project Solution Architects follow all aspects of the Enterprise Technical Solution Architecture Process from initiation to closure;
m) Provide architectural consulting expertise, direction, and assistance to systems analysts, IT Cloud engineers, and other systems architects;
n) Manage the schedule of reviews that need to take place for projects that are in progress;

o) Manage the portfolio of projects engaged with enterprise information architecture; and p) Responsible for guidance on High Level Solutions approach and overall Enterprise Information Solution Architecture patterns.
Minimum Qualification:
a) Degree/diploma in Computer Science, Computer Engineering, Information Technology or equivalent b) Previous relevant experience in the role c) Proficiency with information technologies in a secure network environment d) Agile/Scrum experience as a Developer or an Architect

Role #35 - Business Analyst
Responsibilities:
a) Develop and document statements of requirements for considered alternatives; b) Perform business analyses of functional requirements to identify information, procedures, and decision flows; c) Evaluate existing procedures and methods, identify and document items such as database content, structure, application subsystems; d) Determine improvements to existing business processes based on analyses and evaluations; e) Map existing business processes as well as changes in processes, based on analyses and evaluations; f) Define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems; g) Establish acceptance test criteria with client; h) Develop and establish service level agreements; i) Assist in the formalization of business process standards; j) Support and use the selected organizational methodologies; k) Assist in the development of organizational methodologies and tools; l) Analysis and development of business success "critical success factors"; m) Analysis and development of architecture requirements design, process development, process mapping and training; n) Responsible for leading other functional staff to define business strategy and processes in support of transformation and change management activities; o) Participate in change impact analysis and change management activities; p) Participate in organizational realignment; q) Coordinate development of training and coordination with other stakeholders; and r) Create presentations and present to various stakeholders and facilitate meetings and discussions.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Certified Business Analysis Professional (CBAP) c) Previous relevant experience as a Business Analyst

Role #36 – Application Developer
Responsibilities:
a) Understand client requirements and how they translate in application features; b) Collaborate with a team of IT professionals to set specifications for new applications; c) Design creative prototypes according to specifications; d) Write high quality source code to program complete applications within deadlines; e) Perform unit and integration testing before launch; f) Conduct functional and non-functional testing; g) Troubleshoot and debug applications; h) Evaluate existing applications to reprogram, update and add new features; and i) Develop technical documents and handbooks to accurately represent application design and code.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Previous relevant experience as an Application Developer

Role #37 - Azure Cloud Application Developer

Responsibilities:

a) Supports the design, build, configuration, testing, deployment, management and optimization of secure web applications, connectors and services in relation to both on prem and Cloud applications in MS Azure;
b) Assist with updates, functionality testing, scripts and reporting;
c) Troubleshooting problems, determining root cause and deploying solutions;
d) Assist other developers, analysts, and designers in conceptualizing and developing programs and applications;
e) Run and monitor software performance tests on new and existing programs for the purposes of correcting errors, isolating areas for improvement, and general debugging;
f) Ensure backup and disaster recovery for all Azure resources;
g) Research and document requirements of software users;
h) Supports the design, build, configuration, testing, deployment, management and optimization of secure web applications, connectors and services in relation to both on prem and Cloud applications in MS Azure;
i) Manage and/or provide guidance to junior developers and research assistants;
j) Recommend, schedule, and perform software improvements and upgrades; and
k) Architect applications for ease of maintenance and longevity.

Minimum Qualification:

a) Degree/diploma in Computer Science, Computer Engineering, Information Technology or equivalent
b) Microsoft Azure Certifications
c) Previous relevant experience in the role
d) Experience in IT related position
e) Experience developing with Cloud APIs
f) Experience deploying and supporting an infrastructure in a Cloud based on Amazon Web Services (AWS), Azure, etc.
g) Multi-threading applications
h) Asynchronous processing of events
i) NoSQL databases like MongoDB
j) Web Services
k) Experience refactoring legacy systems for Cloud
l) Agile/ Scrum experience
m) Microsoft Certified Azure Developer Associate or equivalent Microsoft web certification
n) Experience in ASP.Net Core and Visual Studio 2017

Role #38 – Quality Assurance (QA) Tester

Responsibilities:

a) Test planning and coordination;
b) Status reporting;
c) Development of test scenarios and test scripts;
d) Establishing and maintaining source and object code libraries for a multi-platform, multi-operating system environment;
e) Establishing software testing procedures for unit test, integration testing and regression testing with emphasis on automating the testing procedures;
f) Establishing and operating "interoperability" testing procedures to ensure that the interaction and co-existence of various software elements, which are proposed to be distributed on the common infrastructure, conform to appropriate organizational standards (e.g. for performance, compatibility, etc.) and have no unforeseen detrimental effects on the shared infrastructure;
g) Establishing a validation and verification capability which assumes functional and performance compliance;
h) Supervision of testing in accordance with the plan;
i) Management and monitoring of test plans for all levels of testing;
j) Management of walkthroughs and reviews related to testing and implementation readiness;
k) Development and maintenance of QA standards and methodologies; and

l) Development of QA/testing manuals, procedures, and performance measurement tools.
Minimum Qualification:
a) Post-secondary degree/diploma in a related field b) Previous relevant experience as a QA tester

11. <u>The following are the specific descriptions for each Role in Service Category #11 - Business Intelligence and Analytics:</u>

Role #39 - Business Intelligence Developer
Responsibilities:
a) Ensure the stability and reliability of data access and data quality across the organization via ongoing database support and maintenance; b) Analyze user requirements for reports, forms, queries, and data extraction; c) Develop and deploy end-user practices and tools for data extraction, queries, and data manipulation in accordance with business processes; d) Provide end-user training as necessary with regards to the effective and efficient use of database tools and resources; e) Monitor database system details within the database, including stored procedures and execution time, and implement efficiency improvements; f) Create and document models for new database development and/or changes to existing ones through data flowcharting; g) Assist with the installation and configuration of relevant network components to ensure database access, consistency, and integrity; h) Respond to and resolve database access and performance issues; i) Advise on the allocation of physical data storage for database systems; j) Develop, implement, and maintain change control and testing processes for modifications to databases; k) Perform database transaction and security audits; l) Identifying, analyzing and documenting user requirements (e.g. data, information, meta data, access, functionality); m) Designing, developing and maintaining data extraction routines that are required to extract data from the source systems; n) Creating and implementing scripts that will be used to create the physical integrated data base structures; o) Maintaining and tuning of databases and implementing backup and recovery plans and processes for data bases; p) Defining, documenting and maintaining the Enterprise Data Warehouse (EDW) environment; and designing, developing and maintaining the On-Line Analytical Processing (OLAP) components of the EDW environment; q) Specifying, evaluating and selecting EDW tools (e.g. Extract, Transform, Load (ETL) software, and other related tools) and specifying the detailed technical architecture; r) Verifying and monitoring the integrated data store to data marts ETL processes and ensuring that the required data is provided in an efficient manner; s) Facilitating interaction between the user area and the EDW delivery teams; t) Developing and maintaining logical and physical data models for the EDW; u) Establishing, maintaining and providing access to the EDW meta data repository; v) Providing technical infrastructure support services; w) Ensuring that the data delivery environment meets the users' requirements for access and response time; x) Developing appropriate training materials for the EDW user population, providing training courses for the BI tool's users and evaluation of the effectiveness of the training activities; y) Identifying the key organization data that should be provided via the EDW environment; z) Developing test strategies and plans for testing the various components of the EDW environment; aa) Performing data analysis and developing reporting tools and protocols; and bb) Assess and cultivate long-term strategic goals for database development in conjunction with end users, managers, clients, and other stakeholders.

Minimum Qualification:
a) Post-secondary diploma/degree in a related field b) Previous relevant experience as a BI/DW Specialist

Role #40 - Data Architect
Responsibilities:
a) Responsible for the overall data architecture, continuous development, operation, and maintenance of data services and analytic tools; b) Acquire stakeholder requirements and envision optimal data solutions that encourage long-term compatibility, scalability and maintainability; c) Design and implement data products including dashboards and visualizations required to meet the organization's objectives; d) Develop and apply standardization methods to integrate data from numerous sources into corporate data systems, ensuring data integrity and interoperability with existing corporate applications and business intelligence solutions; e) Apply data science techniques for regression and clustering; f) Manage the BI dependency plan, job scheduling and product release-cycle; g) Monitor performance and business use of data systems to identify areas of opportunities for optimization and enhancements; h) Monitor industry trends, identifying and evaluating emerging data technologies, services, standards and strategies; and i) Promote the benefit of standardized business intelligence tools and methodologies across the organization.
Minimum Qualification:
a) University degree in a related field b) Certification related to Business Intelligence c) Previous relevant experience as a BI/DW Specialist

Role #41 - Data Scientist
Responsibilities:
a) Work closely with statisticians to identify, design, and build appropriate datasets for complex experiments; b) Establish links across existing data sources and find new, interesting mash-ups; c) Develop algorithms and predictive models to solve critical business problems; d) Develop tools and libraries that will help analytics team members more efficiently interface with huge amounts of data; e) Create informative visualizations that intuitively display large amounts of data and/or complex relationships; f) Drive the collection of new data and the refinement of existing data sources; g) Analyze large, noisy datasets and identify meaningful patterns that provide actionable results; h) Create data mining and analytics architectures, coding standards, statistical reporting, and data analysis methodologies; i) Coordinate data resource requirements between analytics team and engineering teams; j) Assist in the development of data management policies and procedures; k) Develop best practices for analytics instrumentation and experimentation; l) Conduct research and make recommendations on big data infrastructure, database technologies, analytics tools, services, protocols, and standards in support of procurement and development efforts; m) Develop and automate new enhanced imputation algorithms; n) Provide and apply quality assurance best practices for data science services across the organization; o) Develop, implement, and maintain change control and testing processes for modifications to algorithms and data analytics; and p) Manage and/or provide guidance to junior members of the analytics team.
Minimum Qualification:
a) College diploma or University degree in the field of Computer Science, Information Systems, or Computer Engineering and/or 12 years equivalent work experience

b) Working technical experience with developing, installing, configuring and supporting multi-terabyte database environments
c) Strong understanding of relational database structures, theories, principles, and practices
d) Hands-on experience with business requirements gathering/analysis
e) Previous relevant data scientist or quantitative modeling experience

[END OF APPENDIX "A-1" (SERVICE STREAM #1: STAFF AUGMENTATION SERVICES, SERVICE CATEGORIES AND ROLES)]

Appendix "A-2"

Service Stream #2: Project Delivery Services,
Service Categories

The following is a list of Service Categories for Service Streams #2 Project Delivery Services applicable to this RFSA:

#	Service Category
1	Strategy
2	Architecture
3	Security and Risk
4	Infrastructure
5	Business Application Solutions
6	Salesforce Development
7	Business Intelligence and Analytics

NOTE TO SUPPLIERS: There are no additional Service Categories being added for this RFSA 2021 Refresh.

Service Category #1 - Strategy
Description:
Strategy projects will contribute to the development of strategies intended to improve services and operations for CDIC. The requested project(s) may include but are not limited to: IT Strategy; Data Strategy; Cloud Strategy; Security Strategy; and Modernization Strategy.

Service Category #2 - Architecture
Description:
Architecture projects will translate organizational goals and objectives into architecture requirements, solutions and changes. The requested project(s) may include but are not limited to: Technology Roadmaps; Solution Architectures; and Enterprise Architectures.

Service Category #3 - Security and Risk
Description:
Security and Risk Projects will assess and manage risks for CDIC's information systems. The requested project(s) may include but are not limited to: Security Assessments and Reviews; Security Management; Risk Audits; Security Audits; Penetration Testing, and Vulnerability Scanning.

Service Category #4 - Infrastructure
Description:
Infrastructure projects will rationalize, standardize and structure CDIC's IS Infrastructure landscape. This incorporates the on and/or off-premise technology that supports CDIC. The requested project(s) may include but are not limited to: Cloud Migration; Asset Management; Infrastructure Modernization/Upgrades; and Business Continuity Planning/Disaster Recovery Planning (BCP/DRP).

Service Category #5 - Business Application Solutions
Description:
Business Application solution projects will identify business problems or opportunities and transform into a new application, upgrade existing applications or provide support for existing applications. The requested project(s) may include, but not limited to: strategizing, designing, developing and managing CDIC's applications based on business user requirements.

Service Category #6 - Salesforce Development
Description:
Salesforce Development projects may include, but not be limited to, assessing business objectives and needs and translate them into solutions in the Salesforce platform. The requested project(s) may, but are not limited to: focus on improving the workflow and user experience, configurations, customization and development of applications.

Service Category #7 - Business Intelligence and Analytics
Description:
Business Intelligence and Analytics initiatives related to the creation of new data products including, but not limited to, dashboards, reports, repositories, machine learning applications, upgrade of existing applications and provision of support for existing applications. The requested project(s) may include, but are not limited to, strategizing, designing, developing and managing CDIC's applications based on business user requirements.

[END OF APPENDIX "A-2" (SERVICE STREAM #2: PROJECT DELIVERY SERVICES, SERVICE CATEGORIES)]

Schedule "B"

Evaluation and Selection Process

Selection Method

Without limiting Section 11, CDIC's Reserved Rights of the RFSA, CDIC may, in its sole and absolute discretion, reject or refuse to consider any Proposal if CDIC determines that the information, statements or supporting material in the Technical Offer or the Financial Offer are inconsistent with, or otherwise fail to respond to, any of the requirements of the RFSA.

NOTE TO SUPPLIERS: CDIC expects Suppliers will only submit one Proposal under the RFSA. Suppliers can do so either as a partnership (i.e., Company AB in partnership) or single entity/Supplier (i.e., Company A), but not both. The same Supplier will not be permitted to submit, or be part of, more than one Proposal.

All Proposals for one or both Service Streams will be examined in accordance with the following process:

A. Annual Qualification Opportunity for Supply Arrangements

Step 1: Confirmation of Compliance with the Mandatory Requirements

During Step 1 evaluation, Proposals will be examined to ensure that they meet the **Mandatory Requirements** described in Schedule "C" (Technical Offer) of the RFSA. Suppliers must ensure that all Mandatory Requirements have been addressed satisfactorily in its Proposal, in order for the Proposal to proceed to Step 2 evaluation. Any Proposal that is not considered by CDIC to be in substantial compliance with all mandatory Proposal requirements and all other Mandatory Requirements may be disqualified.

Step 1 will consist of a review of Technical Offers for compliance with the **Mandatory Requirements** described in Schedule "C" (Technical Offer) of the RFSA, to confirm that the information, statements and supporting material in the Supplier's Technical Offer substantiate a compliant response. Subject to CDIC's reserved rights (including those in Section 11, CDIC's Reserved Rights), Mandatory Requirements will be confirmed on a pass or fail basis, and Technical Offers that do not comply with any Mandatory Requirement will be considered non-compliant and will receive no further consideration.

a) Schedule "C" (Technical Offer)
As part of Step 1, CDIC will review the Supplier's Proposal to identify if Schedule "C" (Technical Offer) has been included in the Proposal.

b) Appendix "C-1" (Technical Offer Form)
As part of Step 1, CDIC will review the Supplier's Proposals to identify if Appendix "C-1" (Technical Offer Form) has been included in the Proposal. The Supplier must provide a detailed Technical Offer Form where the Supplier's business experience and expertise will be evaluated as per the instructions and guidelines set out in Schedule "C" (Technical Offer) and in Appendix "C-1" (Technical Offer Form).

c) Appendix "C-2" (Reference Engagement Form)
As part of Step 1, CDIC will review the Supplier's Proposal to identify if Reference Engagement Forms for each Service Category for which the Supplier is offering have been included.

For clarity, the Supplier must provide three (3) completed Reference Engagement Forms for each Service Category being offered under a Service Stream in order for the Supplier's offer for that Service Category to be qualified. If the Supplier does not include three (3) completed Reference Engagement Forms for each Service Category, including for any Service Category with only one Role, its offer for that Service Category will be disqualified.

Suppliers must qualify for at least one Service Category under a Service Stream to be qualified for the Service Stream.

d) Schedule "D" (Financial Offer)
As part of Step 1, CDIC will review the Supplier's Proposal to identify if Schedule "D" (Financial Offer) has been included in the Proposal.

e) Appendix "D-1" (Financial Offer for Service Stream #1)
Supplier qualifying for a Service Category **ONLY** under Service Stream #1 must complete and submit Appendix "D-1" (Financial Offer for Service Stream #1), as applicable.

Step 2: Evaluation of Rated Requirements – Technical Offer (100 Points)

Step 2 will consist of an evaluation of the business experience and expertise of the Supplier as it relates to resources planning.

a) Technical Offer
All Suppliers must submit one (1) Appendix "C-1" (Technical Offer Form), which will be evaluated based on the Supplier's responses to the Rated Requirements provided in the form.

In Step 2, the Supplier will be evaluated on how the Supplier will provide a team of qualified resources when requested by CDIC. This step will also evaluate the methodology used by the Supplier to obtain and manage resources.

The maximum points allocated for Step 2 is **100** Points. A minimum score of **70 points (70%)** is required in order for the Proposal to receive a "pass" for Step 2 and proceed to Step 3 of the evaluation process (see Evaluation Point Allocation Chart in evaluation Step 4, below).

Any Proposal that scores less than the **70 points** required for Step 2 will receive a "fail" and will not proceed to Step 3 of the evaluation process.

Step 3: Evaluation of Rated Requirements –Technical Experience and Expertise - Reference Engagements (300 Points)

Step 3 will consist of an evaluation of the Supplier's (not an individual resource's) Reference Engagements as they relate to the technical experience and expertise for the Service Category being proposed in the Supplier's Proposal.

In Step 3, each Service Category will be evaluated separately and independently from another.

NOTE: All Suppliers are required to submit three (3) Reference Engagement Forms per Service Category in which they are bidding.

The maximum total points allocation for Step 3 for each Service Category under a Service Stream is **300 points** (100 points for each Reference Engagement Form). Each Service Category in a Proposal must score a minimum of **210 points (70%)** to receive a "pass" for that Service Category. Any Service Category that does not receive a minimum score of **210 points** will receive a "fail" for that Service Category only, and the Supplier will not be qualified for that Service Category.

In addition, each Reference Engagement Form in a Proposal must score a minimum of **70 points (70%)** to receive a "pass" for that Service Category. A Reference Engagement Form for any Service Category that does not receive a minimum score of **70 points** will receive a "fail" for that Service Category only and the Supplier will not be qualified for that Service Category.

For a Supplier to qualify for a Service Stream, they must qualify for at least one Service Category under that Service Stream.

a) Reference Engagement Form

The Supplier must provide three (3) completed Reference Engagement Forms for the Service Category being offered (**one Reference Engagement Form for each of three (3) independent and distinct**

Engagements), according to the instructions contained in the form, including for any Service Category with only one Role.

The Supplier must provide details in each of the three (3) Reference Engagement Forms of its experience and expertise as it relates to the particular Service Category under a Service Stream for which the Supplier is submitting an offer. Scoring of the Reference Engagement Form will be based on how well the Proposal demonstrates the Supplier's technical experience and expertise in relation to the requirements in the RFSA and the level of detail of the Reference Engagement Forms provided. Information provided elsewhere in the Proposal may not be considered in the evaluation of Step 3 of this RFSA.

The information provided in the Reference Engagement Form must reflect Engagements the Supplier has **completed after January 1, 2015,** and prior to the Proposal Submission Deadline. Any Engagement with a completion date prior to January 1, 2015, or after the Proposal Submission Deadline will not be considered for evaluation and will be disqualified. The Engagements must directly relate to the Service Category for which the Supplier wishes to be qualified in the Service Stream as described in Schedule "A" (Statement of Work) of this RFSA and offered in the Supplier's Proposal.

If a Supplier submits fewer than the three (3) Reference Engagement Forms required for a particular Service Category in a Service Stream, the Supplier will not be qualified for that particular Service Category.

Each Service Category will receive an individual score for the Reference Engagement Forms that the Supplier has provided to demonstrate the Supplier's ability to provide Services in the particular Service Category.

Each of the three (3) Reference Engagement Forms required will be scored independently, and each will have a maximum score of 100 points. The scores from each of the three (3) Reference Engagement Forms for a particular Service Category will be added together to determine the total score for that Service Category.

For example, the three (3) Reference Engagement Forms submitted for a particular Service Category in Service Stream #1, receive scores of 80 points, 85 points and 90 points. The three (3) scores will be added together to achieve a total score of 255 points for that particular Service Category in Service Stream #1 and will be considered to have obtained the minimum score of 210 points required for that particular Service Category in Service Stream #1.

As each Service Category will be scored separately, it is possible for a Proposal to pass the Step 3 evaluation for one particular Service Category ("X") but not for another Service Category ("Y"), if:

(a) the three (3) Reference Engagement Forms provided for the Service Category ("Y"), do not achieve in total, the minimum point score (210 points) required; or

(b) one (1) of the three (3) Reference Engagement Forms provided for Service Category ("Y"), does not achieve, the minimum point score (70 points) required.

b) Evaluation

Step 3 evaluation will be conducted in two stages:

- Stage 1 - (Evaluation of each Reference Engagement Form)
- Stage 2 - (Cumulative Total Score of all Reference Engagement Forms)

i. **Stage 1 – Evaluation of Reference Engagement Forms (Appendix "C-2")**

In this evaluation stage, each Reference Engagement Form will be evaluated separately and individually.

The maximum score for each Reference Engagement Form is 100 points.

The Supplier must demonstrate its ability to provide services in one or more Service Category under one or both of the two (2) Service Streams in Schedule "A" (Statement of Work). Three (3) Reference Engagement Forms are required for each Service Category. Each Reference Engagement Form is allocated up to 100 points. Therefore, a total maximum score of 300 points is allocated for each Service Category. A Reference Engagement Form must receive a minimum of 70 points for each Service Category in order to be considered for that Service Category.

Example Evaluation Scenario for Illustration Purposes

REFERENCE ENGAGEMENT (REF)	SERVICE CATEGORY (SC)	
	SC#1	SC#2
REF #1	100	80
REF #2	**40**	90
REF #3	80	75
PASS/FAIL	**Fail**	Pass

NOTE: A Supplier must be successful in one or both of the two (2) Service Streams by qualifying in at least one Service Category under a Service Stream to proceed further in the evaluation process.

ii. **Stage 2 - Cumulative Total Score of all three (3) Reference Engagement Forms**

The scores for each of the three (3) Reference Engagement Forms that receive a "pass" in Stage 1, will be added together to determine the cumulative total score for the Service Category. A Proposal that achieves a minimum cumulative total score of 210 points will pass Step 3.

Scenario #1

REFERENCE ENGAGEMENT FORMS (REF) For SC#1 Under Service Stream #1	TOTAL POINTS (per RE)	PASS / FAIL	Cumulative Total Score for SC#1	Step 3 Result for SC#1
REF #1	77	Pass	77 + 84 + 90 = 251	Pass
REF #2	84	Pass		
REF #3	90	Pass		

Scenario #2

REFERENCE ENGAGEMENT FORMS (REF) For SC#1 Under Service Stream #1	TOTAL POINTS (per RE)	PASS / FAIL	Cumulative Total Score for SC#1	Step 3 Result for SC#1
REF #1	60	Fail	60 + 75 + 70 = 205	Fail
REF #2	75	Pass		
REF #3	70	Pass		

Scenario #3

REFERENCE ENGAGEMENT FORMS (REF) For SC#1 Under Service Stream #1	TOTAL POINTS (per RE)	PASS / FAIL	Cumulative Total Score for SC#1	Step 3 Result for SC#1
REF #1	75	Pass	75 + 65 + 90 = 230	Fail
REF #2	65	Fail		
REF #3	90	Pass		

Step 4: Selection of Successful Suppliers

At the conclusion of Step 3 (Evaluation of Rated Requirements), subject to, and without limiting any other provision in this RFSA, including but not limited to, Section 11, CDIC's Reserved Rights, a recommendation may be made by CDIC to award an agreement to each Supplier that is successful in one or both Service Stream(s) to provide Services in the Service Category that achieved a "pass" in Stage 3. If the recommendation is approved, CDIC will award the agreement and will enter into the agreement with the Supplier in accordance with this RFSA.

B. Subsequent Annual Qualification Opportunities for Supply Arrangements

An annual notice re-inviting interested suppliers to submit proposals for consideration and potential award of a Supply Arrangement will be published on the second anniversary of the Initial Supply Arrangements, and in the event CDIC exercises available options, on the third and on the fourth anniversary, as may be applicable, and Suppliers will be allowed to submit proposals at any time. However, proposals received after the Deadline for Proposals will be evaluated with the next scheduled annual evaluation. Proposals received will be evaluated in accordance with the process described in Part A above.

NOTE TO EXISTING QUALIFIED SUPPLY ARRANGEMENT HOLDERS:

Qualified Supply Arrangement Holders are not required to resubmit proposals in response to annual qualification opportunities unless such Supply Arrangement Holders are seeking to add one or more roles and/or Service Categories to its Supply Arrangement, in which event, a complete Technical Offer (but limited to those new roles and/or Service Categories) should be submitted for evaluation by CDIC.

Evaluation Point Allocation Chart

The following tables show a summary of the evaluation steps and methodology for this RFSA:

Steps	Evaluation Criteria	Maximum Points	Minimum Points Required
1	**Mandatory Proposal Requirements**	Pass	**Pass**
2	**Technical Offer Form** Business Experience and Expertise in Resource Planning (Rated) **(Appendix "C-1")**	**100** points	**Pass** **70** points (70%)
3	**Reference Engagement Forms** Technical Experience and Expertise (Rated) **(Appendix "C-2")**	**300** points (100 points for each Reference Engagement Form)	**Pass** **Total of 210** points (70 minimum points for each Reference Engagement Form)

Scoring Methodology

The following is the basis for the scoring method that will be applied to the rated requirements in Appendix "C-1" (Technical Offer Form) and Appendix "C-2" (Reference Engagement Form):

Score	Rationale
5	Exceptional, fully meets and/or exceeds CDIC's requirement. No weaknesses exist. A comprehensive response with no significant gaps.
4	Very Good, substantially meets CDIC's requirement. Strengths exceed weaknesses, and weaknesses are easily correctable.
3	Acceptable, meets the basic requirement of CDIC. There may be strengths or weaknesses, or both. Weaknesses do not significantly impact the requirements and are correctable.
2	Marginal, falls short of meeting the basic requirement of CDIC. Weaknesses exceed strengths and will be difficult to correct.
1	Unacceptable, minimal response, e.g., statement of compliance with no substantiation. Noted deficiencies are expected to be very difficult to correct or are not correctable.
0	Unresponsive, no relevant response / unsatisfactory.

[END OF SCHEDULE "B" (EVALUATION AND SELECTION PROCESS)]

Schedule "C"

Technical Offer

Technical Offer should be accompanied by Appendix "C-1" (Technical Offer Form) and all applicable Appendix "C-2" (Reference Engagement Form(s)), for each Service Category being offered under the Service Stream(s).

TECHNICAL OFFER

LEGAL NAME OF SUPPLIER: _____

ADDRESS: _____

CONTACT NAME: _____

TELEPHONE: _____

EMAIL: _____

SOLICITATION NUMBER: **CDIC RFSA 2020-2842 – 2021 REFRESH**

TITLE: **Information Technology Staff Augmentation and Project Delivery Services**

1. The undersigned, as the authorized representative of the supplier (hereinafter referred to as the "**Bidder")** hereby offers to the Canada Deposit Insurance Corporation ("**CDIC**") all necessary goods, services, labour, superintendence, supplies and facilities, and pursuant to the above solicitation, warrants and certifies:

   i) It has not, directly or indirectly, paid or agreed to pay, and will not, directly or indirectly, pay, a contingency fee to any individual for the solicitation, negotiation or obtaining of the Agreement if the payment of the fee would require the individual to file a return under section 5 of the *Lobbying Act*; and

   ii) It has not been convicted of an offence under section 121, 124 or 418 of the *Criminal Code* other than an offence for which a pardon has been granted.

   iii) That all personnel under the resulting Contract who will access CDIC workplaces where they may come into contact with employees (the "CDIC assigned personnel") will be:

      a) fully vaccinated against COVID-19 with Health-Canada-approved vaccine(s); or
      b) for CDIC assigned personnel that are unable to be vaccinated due to certified medical contraindication, religion or other prohibited grounds of discrimination under the *Canadian Human Rights Act*, subject to accommodation and mitigation measures that have been presented to and approved by CDIC;

   until such time that CDIC indicates that the vaccination requirements are no longer in effect.

   iv) It has notified all CDIC assigned personnel of the vaccination requirements and certifies to their compliance with this requirement.

2. Ability to Provide Deliverables

   The Bidder has carefully examined the RFSA documents and has a clear and comprehensive knowledge of the Services required. The Bidder represents and warrants its ability to provide the Services in accordance with the requirements of the RFSA for the rates set out in its proposal.

3. Acknowledgment of Non-Binding Procurement Process

The Bidder acknowledges that the RFSA process will be governed by the terms and conditions of the RFSA, and that, among other things, such terms and conditions confirm that this procurement process does not constitute a formal, legally binding bidding process (and for greater certainty, does not give rise to a contract, a bidding process contract), and that no legal relationship or obligation regarding the procurement of any good or service will be created between CDIC and the Bidder unless and until CDIC and the Bidder execute a written agreement for the Services.

4. No Prohibited Conduct

The Bidder declares that it has not engaged in any conduct prohibited by this RFSA.

5. Conflict of Interest

The Bidder must declare all potential Conflicts of Interest. This includes disclosing the names and all pertinent details of all individuals (employees, advisers, or individuals acting in any other capacity) who (a) participated in the preparation of the proposal; **AND** (b) were employees of CDIC within twelve (12) months prior to the Deadline for Proposals.

If the box below is left blank, the Bidder will be deemed to declare that (a) there was no Conflict of Interest in preparing its proposal; and (b) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the RFSA.

Otherwise, if the statement below applies, check the box.

☐ The Bidder declares that there is an actual or potential Conflict of Interest relating to the preparation of its proposal, and/or the Bidder foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the RFSA.

If the Bidder declares an actual or potential Conflict of Interest by marking the box above, the Bidder must set out below details of the actual or potential Conflict of Interest:

_____

_____

_____

6. Disclosure of Information

The Bidder hereby agrees that any information provided in this proposal, even if it is identified as being supplied in confidence, may be disclosed where required by law or by order of a court or tribunal. The Bidder hereby consents to the disclosure, on a confidential basis, of this proposal by CDIC to the advisers retained by CDIC to advise or assist with the RFSA process, including with respect to the evaluation this proposal.

By signing this Form the Bidder represents that the above information is true as of the date indicated below and will continue to be true for the duration of any resulting Contract. Bidder understands that the certifications provided to CDIC are subject to verification at all times, and further understands that CDIC will declare a contractor in default, if a certification is found to be untrue, whether made knowingly or unknowingly, during the solicitation or contract period. CDIC reserves the right to ask for additional information to verify the certifications. Failure to comply with any request or requirement imposed by CDIC will constitute a default under any resulting Contract.

Bidder Signature	Date
Print Name	Title

I have authority to bind the Bidder.

OFFERS WHICH DO NOT CONTAIN THE REQUESTED DOCUMENTATION MAY BE DEEMED NON-COMPLIANT.

Technical Offer Requirements and Evaluation

A. Mandatory Requirements

M1.	Supplier must submit a completed Schedule "C" (Technical Offer).
M2.	Supplier must complete and submit the Appendix "C-1" (Technical Offer Form) – One per Proposal.
M3.	Supplier must complete and submit three (3) Reference Engagement Forms (see Appendix "C-2" (Reference Engagement Form)) for each Service Category being offered under the applicable Service Stream.
M4.	Suppliers must submit a completed Schedule "D" (Financial Offer).

NOTE: The following Mandatory Requirement is ONLY applicable to Suppliers submitting Reference Engagement Forms for a Service Category under Service Stream #1:

M5.	Supplier qualifying for a Service Category under Service Stream #1 must complete and submit Appendix "D-1" (Financial Offer for Service Stream #1) as applicable

B. Technical Offer Requirements

CDIC will evaluate the Supplier's Technical Offer and assign points in respect of each of the Service Stream(s) the Supplier is offering as part of its Proposal based in part on how the Supplier demonstrates its knowledge and experience in response to the Rated Requirements identified in Appendix "C-1" (Technical Offer Form), below.

For clarity, the detail and information requested in each Rated Requirement should be provided for each of the Service Stream(s) the Supplier is offering as part of its Proposal.

All requested information should be provided in Appendix "C-1" (Technical Offer Form), below.

[END OF SCHEDULE "C" (TECHNICAL OFFER)]

Appendix "C-1"

Technical Offer Form

Instructions: The bidder must not alter the format of the table below in any way, other than to remove highlighted text and add hard returns to provide responses. Columns and rows are not to be added or deleted. The maximum number of words is an absolute maximum and should be adhered to whether a bidder is submitting for one or both Service Streams.

1. Supplier Information – Supplier should provide the following information (Not Rated):	
a) Supplier's Legal Name:	[Insert legal name]
b) Number of years the Supplier has been in business:	[Insert years in business]
c) Number of employees employed by the Supplier (identify the number of full-time, part-time and contract personnel):	
(Maximum of 200 words)	
d) Description of the corporate history of Supplier, including any acquisitions or divestitures over the last ten (10) years:	
(Maximum of 500 words)	
e) Location of each of the Supplier's offices, including number of staff at each location and their primary functions:	
(Maximum of 500 words)	

2. The Supplier must identify the Service Stream(s) it will offer by placing an in one or both of the applicable boxes.
☐ **1. Service Stream #1: Staff Augmentation Services**
☐ **2. Service Stream #2: Project Delivery Services**
** NOTE: Suppliers must identify each Service Category for which they will be offering in Appendix "C-2".*

3. Rated Requirements – (Maximum Total Points - 100)

RR #1 – Organizational Experience – (Maximum assigned points – 30)

Supplier should clearly describe the organization's knowledge, qualifications and expertise in relation to the proposed Service Stream(s) the Supplier is offering as part of its Proposal.

Supplier should provide, at a minimum, a clear description of how such knowledge, qualifications and expertise are aligned with CDIC's requirements for each Service Stream(s) the Supplier will be offering as part of its Proposal.

A #1: *(Maximum of 1,000 words)*

RR #2 – Understanding and Approach – (Maximum assigned points – 10)

Supplier should describe its understanding of CDIC's requirements in relation to the Service Stream(s) the Supplier is offering as part of its Proposal, and the Supplier's approach to meeting CDIC's requirements.

In its description, Supplier should clearly demonstrate:

a) *How the Supplier plans to establish and maintain an effective working relationship with CDIC;*

b) *How the Supplier will collaborate with CDIC and manage feedback and changes; and*

c) *How the Supplier will handle any issues that may arise between the Supplier and CDIC.*

A #2 *(Maximum of 500 words)*

RR #3 – Key Personnel Qualifications – (Maximum assigned points – 10)

In relation to the services described under the Service Stream(s) the Supplier is offering as part of its Proposal, the Supplier should:

a) *Clearly identify the proposed key client relationship lead(s), including who will serve as the key point of contact for each applicable Service Stream, and clearly describe any other roles and resources that would be involved in providing such services to CDIC;*

b) *For the key client relationship lead(s) that the Supplier proposes to assign to CDIC for the delivery of the Services identified for each respective Service Stream, and for any proposed alternate, provide a resumé that includes the number of years of experience providing services such as those required for the engagement with CDIC, including specific examples of experience; and*

c) *Clearly identify and describe the Supplier's approach to maintaining its relationship with CDIC in the event that a change of key client relationship lead(s) and/or key point of contact occurs, on either an interim or an ongoing basis.*

A #3 *(Maximum of 500 words, excluding resumé(s))*

RR #4 – Ongoing Access to Resources – (Maximum assigned points – 10)

Supplier should clearly describe for each of the Service Stream(s) the Supplier is offering as part of its Proposal:

a) *How the Supplier will retain ongoing access to qualified information technology resources to meet immediate and future CDIC requirements.*

b) How the Supplier will cover for any absences and/or departures of resources during the performance of the Services. The Supplier should clearly describe its current resource management framework and explain how it will be applied.

A #4 *(Maximum of 500 words)*

RR #5 – Performance / Service Levels – (Maximum assigned points – 10)

Supplier should clearly describe for each of the Service Stream(s) the Supplier is offering as part of its Proposal, the processes the Supplier has in place that will measure the Supplier's organization's performance and service levels to meet CDIC's requirements, including such processes for any subcontractors (if applicable).

A #5 *(Maximum of 500 words)*

RR #6 – Quality Assurance – (Maximum assigned points – 10)

Supplier should clearly describe for each of the Service Stream(s) the Supplier will be offering as part of its Proposal:

a) Approach to quality assurance for the performance of the Services for each proposed Service Stream; and

b) How the quality assurance approach will be consistent throughout the duration of the Supply Arrangement for each proposed Service Stream, including such approach for any subcontractors (if applicable).

A #6 *(Maximum of 500 words)*

RR #7 – Information Security – (Maximum assigned points – 20) *Supplier should clearly describe methodology and approach to collecting CDIC data and maintaining data security throughout the duration of the Supply Arrangement, including reassurances that CDIC collected data will only be stored in Canada.*
A #7 *(Maximum of 500 words)*

[END OF APPENDIX "C-1" (TECHNICAL OFFER FORM)]

Appendix "C-2"

Reference Engagement Form Requirements

1. Reference Engagement Form Requirements / Instructions

NOTE: To be eligible, Reference Engagement Forms must profile only Engagements that were completed after January 1, 2015, and prior to the Proposal Submission Deadline. Any Engagement with a completion date prior to January 1, 2015, or after the Proposal Submission Deadline will not be considered for evaluation and will be disqualified.

1.1. The Reference Engagement Form below must be completed for each Reference Engagement being profiled. In order to ensure that the Supplier has an opportunity to attain a high score for the Reference Engagement Form, detailed responses must be provided to each of the Rated Requirements set out in the Reference Engagement Form.

1.2. A separate Reference Engagement Form must be used for each proposed Service Category under a Service Stream using only the Service Category name referred in this RFSA for which the Supplier wishes to be qualified. The Supplier must identify, in Section 1 of the Reference Engagement Form, both the Service Stream and Service Category to which the Reference Engagement Form applies by placing an (X) in the box beside the name of the Service Stream and the applicable Service Category to which the Reference Engagement Form relates, respectively. If the Supplier places an (X) in more than one box, CDIC will only evaluate the Reference Engagement indicated by the first box in which an (X) appears**. For a Service Category under Service Stream #1 ONLY, Suppliers should also identify at least one (or more) relevant Role(s) by placing an (X) in the box beside the name of the Role(s).**

In order to meet Step 3: Evaluation of Rated Requirements – Technical Experience and Expertise, of Schedule "B" (Evaluation and Selection Process) (referred to herein as "Step 3 Requirements"), a Supplier that submits a Proposal for any of the two (2) Service Streams shall include in its Proposal three (3) Reference Engagement Forms for each Service Category being offered under a Service Stream.

For example:

(i) A Supplier submitting a Proposal for Service Category #1 (Advisory Services) and Service Category #5 (Technical Support) under Service Stream #1, must, in order to meet Step 3 Requirements for a Service Category, submit three (3) Reference Engagement Forms for each Service Category– for a total of six (6) Reference Engagement Forms.

(ii) A Supplier submitting a Proposal for **all** eleven (11) Service Categories under Service Stream #1 and **all** seven (7) Service Categories under Service Stream #2 must, in order to meet Step 3 Requirements for all of the Service Categories, submit three (3) Reference Engagement Forms for each Service Category – for a total of fifty-four (54) Reference Engagement Forms.

1.3. Only three (3) Reference Engagement Forms may be submitted for each Service Category. If a Supplier submits more than three (3) Reference Engagement Forms for the same Service Category in its Proposal, CDIC will only evaluate the first three (3) Reference Engagement Forms submitted for that Service Category, in the order in which they appear in the Proposal.

1.4. A Supplier **may not** submit the same Reference Engagement Form for more than one (1) Service Category. Each of the three (3) Reference Engagement Forms submitted for a Service Category must be for different Engagements. Also, **an Engagement may only be profiled once in a Supplier's Proposal**. If the Supplier does profile the same Engagement more than once, CDIC will only evaluate the Engagement in the first Reference Engagement Form in which it appears.

NOTE TO SUPPLIERS: Suppliers may provide the same Engagement for more than one (1) Service Category. However, each of the three (3) Reference Engagement Forms submitted for a given Service Category must be for different Engagements. For greater clarity, an Engagement may only be profiled once per Service Category being offered. If the Supplier does provide the same Engagement more than

once for a Service Category, its offer for that Service Category will be disqualified.

Suppliers who choose to provide the same Engagement for more than one (1) Service Category in their Proposal, should ensure the details of the Reference Engagement Form are relevant to each Service Category for which the Reference Engagement Form is provided. Simply "copying and pasting" the details of the Engagement and/or providing the same Reference Engagement Form for more than one (1) Service Category with no clear changes made to address the requirements of the Service Category for which the Engagement is provided, may lead to a lower score for any such Service Category being offered.

1.5. The dollar value of each Reference Engagement that is profiled must have a minimum value of $25,000 (CAD). Any Reference Engagement with a value under $25,000 will not be considered for evaluation and will be disqualified.

1.6. The "**Supplier's Legal Name"** provided in the Reference Engagement Form should be the same legal name provided in Schedule "C" (Technical Offer).

The Supplier should carefully review and follow the instructions set out in the RFSA, including, without limitation, in this Appendix "C-2" (Reference Engagement Form) when completing a Reference Engagement Form. The Supplier should consider the definition of Reference Engagement, in Section 4, Summary of Key RFSA Dates and Defined Terms in this RFSA, and the description of eligible Engagements contained therein.

Reference Engagement Forms submitted in the Supplier's Proposal should detail a Reference Engagement that has been completed and that a Supplier has chosen to profile as described in the evaluation of Step 3 Requirements. Reference Engagements that are eligible to be profiled are only those Reference Engagements carried out by:

(a) the Supplier, where the Supplier retained responsibility for and control over the work of its personnel and/or its subcontractors on the Reference Engagement; or

(b) if the Supplier is a partnership, any partner forming part of the partnership, where that partner retained responsibility for and control over the work of its personnel and/or its subcontractors in relation to the Reference Engagement.

NOTE TO SUPPLIERS: Suppliers are not required to submit separate Reference Engagements Forms for each of the forty-one (41) Roles under Service Stream #1 or map each Role to their specific responsibilities/ qualifications. Suppliers that qualify for a specific Service Category will qualify for ALL Roles for which they have provided a rate in Appendix "D-1" (Financial Offer for Service Stream #1).

1.7. The Supplier **must not** indicate "on-going" or other similar wording to describe a Reference Engagement that has not yet been completed as the Engagement End Date in the Reference Engagement Form. A firm completion date (i.e., the day, month and year) must be shown for the Reference Engagement that has been completed. Any Reference Engagement Form with an "on-going" completion date will not be considered for evaluation.

A Reference Engagement that has deliverables which include on-going maintenance and support may be profiled; however, only the **completed** portion of the deliverables is considered by CDIC to be eligible to be profiled**.** A Reference Engagement that is still on-going as at the **Proposal Submission Deadline** is not considered by CDIC to be eligible to be profiled and **will not** be considered for evaluation.

NOTE TO SUPPLIERS: A Supplier would be able to profile a multi-year contract and/or ongoing engagement as long as the Supplier can clearly demonstrate that a portion of the relevant deliverables have been completed prior to the Proposal Submission Deadline.

1.8. Engagement Profiles may be for Reference Engagements conducted for clients in either the public or private sector.

NOTE TO SUPPLIERS: The Reference Engagements are not limited to Engagements completed in Canada. Suppliers should provide the applicable information requested that accurately describes their organization as it relates to providing the Services required by CDIC as described in the RFSA.

Private sector related Reference Engagements are not limited to clients within the financial sector/services.

1.9. Total level of effort for a given Service Category within a Reference Engagement Form must be a minimum of 20 working days (7 hours equals 1 working day) level of effort

1.10. Each Reference Engagement Form provided must thoroughly demonstrate the Supplier's experience and ability in performing the Services with respect to the particular Service Category for which it wishes to be qualified within the Service Stream being proposed. The Supplier must describe **in detail** the evidence of skills for the Service Category being profiled. Suppliers can demonstrate their experience/skills by identifying and clearly describing specific experience with at least one Role under the Service Category.

1.11. Without limiting the reserved right of CDIC to check references other than those provided by the Supplier, CDIC, in its sole discretion, may, during the RFSA evaluation process, confirm the Supplier's experience and/or ability to undertake the Engagement/provide the Services required and described in the Supplier's Proposal by contacting the named Engagement reference identified in the Reference Engagement Form to verify the information provided.

Reference Engagement Form

NOTE: Three (3) Reference Engagement Forms to be completed for each Service Category.

Instructions: The bidder must not alter the format of the table below in any way, other than to remove highlighted text and add hard returns to provide responses. Columns and rows are not to be added or deleted. The maximum number of words is an absolute maximum and should be adhered to whether a bidder is submitting for one or both Service Streams.

Supplier's Legal Name:	[Insert legal name]

1. The Supplier must identify the Service Stream and Service Category profiled in this Reference Engagement (ONLY 1 Service Stream and Service Category per Reference Engagement) by placing an in the applicable box.

Service Stream	
☐ **1. Service Stream #1: Staff Augmentation Services**	☐ **2. Service Stream #2: Project Delivery Services**

Service Category (SC)	
☐ **1. Advisory Services**	☐ **1. Strategy**
☐ **2. Project Management**	☐ **2. Architecture**
☐ **3. Cyber Security**	☐ **3. Security and Risk**
☐ **4. Enterprise Technology**	☐ **4. Infrastructure**
☐ **5. Technical Support**	☐ **5. Business Application Solutions**
☐ **6. SharePoint Support**	☐ **6. Salesforce Development**
☐ **7. Salesforce Support**	☐ **7. Business Intelligence and Analytics**
☐ **8. Alteryx Support**	
☐ **9. Agile Application Delivery**	
☐ **10. Application Development**	
☐ **11. Business Intelligence and Analytics**	

For a Service Category under Service Stream # 1 ONLY, the Supplier should identify one or more Role(s) profiled in this Reference Engagement by placing an in the applicable box.

☐ **1. IT Executive Strategic Advisor (SC#1)**	☐ **22. Security Incident Responder (SC#5)**
☐ **2. Data Strategy Advisor (SC#1)**	☐ **23. Infrastructure Operations and Support (SC#5)**
☐ **3. Project Management Office Lead (SC#2)**	☐ **24. Technical Writer / Trainer / Courseware Author (Developer) (SC#5)**
☐ **4. Project Manager (SC#2)**	☐ **25. SharePoint Online Administrator (SC#6)**
☐ **5. Project Administrator (SC#2)**	☐ **26. SharePoint Online Architect (SC#6)**
☐ **6. Security Analyst (SC#3)**	☐ **27. SharePoint Online Developer (SC#6)**
☐ **7. Application Security Administrator (SC#3)**	☐ **28. Salesforce Developer (SC#7)**
☐ **8. IT Security Architect (SC#3)**	☐ **29. Salesforce Tester (SC#7)**
☐ **9. Ethical / White Hat Hacker (SC#3)**	☐ **30. Salesforce Administrator (SC#7)**
☐ **10. Azure Security Architect (SC#3)**	☐ **31. Alteryx Developer (SC#8)**
☐ **11. Azure Security Administrator (SC#3)**	☐ **32. Scrum Master (SC#9)**
☐ **12. Storage Admin / Virtualization Architect SC#4)**	☐ **33. Agile Team Coach (SC#9)**
☐ **13. Systems Architect (SC#4)**	☐ **34. Solution Architect (SC#10)**
☐ **14. Azure Architect (SC#4)**	☐ **35. Business Analyst (SC#10)**
☐ **15. Azure Administrator (SC#4)**	☐ **36. Application Developer (SC#10)**
☐ **16. Azure Data Base Administrator (SC#4)**	
☐ **17. Webmaster (SC#4)**	

☐ **18. Application Support Specialist (SC#5)** ☐ **19. Deskside Technical Support Analyst (SC#5)** ☐ **20. Service Desk Analyst (SC#5)** ☐ **21. IT Service Management Specialist (SC#5)**	☐ **37. Azure Cloud Application Developer (SC#10)** ☐ **38. Quality Assurance (QA)Tester (SC#10)** ☐ **39. Business Intelligence Developer (SC#11)** ☐ **40. Data Architect (SC#11)** ☐ **41. Data Scientist (SC#11)**
The following is a list of eight (8) additional Roles for Service Stream #1: Staff Augmentation Services, applicable to this RFSA 2021 Refresh.	
☐ **42. IT Service Manager (SC#2)** ☐ **43. Cyber Forensics Specialist (SC#3)** ☐ **44. Security Engineer (Application/Network) (SC#3)** ☐ **45. SOC Analyst (SC#3)**	☐ **46. SOC Lead/Manager (SC#3)** ☐ **47. Cloud Security Specialist (SC#3)** ☐ **48. Security Administrator (SC#3)** ☐ **49. Governance Risk and Compliance Analyst (SC#3)**

2. Engagement Reference - Client (Company) Contact Information	
Client (Company) Name:	
Client (Company) Address:	
Client Contact Person Name:	
Title:	
Telephone #:	
Email:	

3. Engagement Profile Details			
Engagement/Project Name:			
Engagement Value:	**$**		
Engagement Start Date: (mm/dd/yyyy) (e.g. 07/01/ 2017)		**Total Level of Effort (Days):** *(7 hours equals 1 working day)*	_____ Days
Engagement End Date: (mm/dd/yyyy) (e.g. 12/31/ 2018)			

4. Technical Experience and Expertise (Maximum assigned points - 100)

RR #4.1 Scope and Type of Services – (Maximum assigned points – 40)

Supplier should clearly describe in detail the scope and type of services provided, including any similarities/relevance between the client and CDIC's organizations.

The details should clearly demonstrate relevance to the scope of the respective Service Category described in Appendix "A-1" and Appendix "A-2", as applicable, for each Service Category under a Service Stream the Supplier is offering as part of its *Proposal*.

NOTE: For a Service Category under Service Stream #1 ONLY, the Supplier should also clearly describe relevance to the scope of at least one Role as described in Appendix "A-1".

A #4.1 [Insert detailed description of services – Maximum of 500 words]

RR #4.2 Client Management – (Maximum assigned points – 15)

Supplier should clearly describe, in detail, how the Engagement was approached by addressing each of the following items:

a) Understanding and delivery of the client's vision;
b) Methodologies and tools used to complete the deliverables;
c) Managing client feedback and changes; and.
d) Ensuring client engagement and involvement.

A #4.2 [Insert detailed description of services – Maximum of 500 words]

RR #4.3 Knowledge Transfer – (Maximum assigned points – 15)

Supplier should clearly describe, in detail, the processes used by the Supplier to transfer knowledge to the client upon completion of this Engagement (e.g. reports, training, user manual):

A #4.3 [Insert detailed description of knowledge transfer - Maximum of 500 words]

RR #4.4 Outcome of Engagement – (Maximum assigned points – 15)

Describe in detail the outcome of this Engagement:

A #4.4 [Insert detailed description of outcome of Engagement - Maximum of 500 words]
RR #4.5 Success Factors – (Maximum assigned points – 15) Describe in detail the critical success factors and how Supplier contributed to achieve the outcome:
A #4.5 [Insert detailed description of success factors - Maximum of 500 words]

[END OF APPENDIX "C-2" (REFERENCE ENGAGEMENT FORM)]

Schedule "D"

Financial Offer

FINANCIAL OFFER

LEGAL NAME OF SUPPLIER: _____

ADDRESS: _____

CONTACT NAME: _____

TELEPHONE #: _____

EMAIL: _____

SOLICITATION NUMBER: **CDIC RFSA 2020-2842 – 2021 REFRESH**

TITLE: **Information Technology Staff Augmentation and Project Delivery Services**

The undersigned supplier (hereinafter referred to as the "**Bidder**") hereby offers to perform and complete the work at the place, and in the manner set out in accordance with the documents specified in the RFSA and any additional documents or information submitted as part of its Technical Offer and at the prices specified herein for Service Stream #1.

1. Place of Residence Information

1.1 Bidder **Resident** of Canada for Canadian tax purposes □

1.2 Bidder **Non-resident** of Canada for Canadian tax purposes □

If not specified, the Bidder will be deemed to represent and warrant that it is a resident of Canada for Canadian tax purposes.

By signing this Form, the Bidder represents that the above information is accurate.

_____ _____

Bidder Signature Date

_____ _____

Print Name Title

I have authority to bind the Bidder.

PROPOSALS WHICH DO NOT CONTAIN THE REQUESTED DOCUMENTATION MAY BE DEEMED NON-COMPLIANT.

Financial Offer Requirements

1. Financial Offer Requirements

1.1 Financial Offers should include Schedule "D" (Financial Offer). For greatly clarity, Appendix "D-1" (Financial Offer for Service Stream #1) is **ONLY** required for Suppliers submitting for one or more Service Category under Service Stream #1. The Supplier must submit Financial Offers in Canadian dollars and exclusive of Canadian Goods and Services Tax (GST), Harmonized Sales Tax (HST), and/or provincial sales taxes (PST), as applicable.

1.2 The Supplier must provide an all-inclusive ceiling rate/price necessary to deliver all Services and Roles related to each Service Category under Service Streams #1, as set out in Schedule "A" (Statement of Work), that the Supplier will be proposing as part of its Proposal and as outlined in Appendix "D-1", which shall be payable as per Appendix "A" of the Professional Services Agreement, attached to the RFSA as Schedule "F" (Form of Professional Services Agreement).

Rates shall include all labour, materials, photocopies, telephone charges, overhead, profit and all other fees, expenses and costs associated with providing the services, as set out in Schedule "A" (Statement of Work), unless expressly excluded by CDIC in Schedule "D" (Financial Offer) and excluding any applicable pre-approved expenses.

NOTE TO SUPPLIERS: The hourly ceiling rates submitted by Suppliers will be the ceiling rates applicable for the term of the resulting agreement, including any optional extension term, if exercised in CDIC's sole and absolute discretion, with no possibility for an increase. As such, it is the Suppliers' responsibility to ensure its rates include amounts for any future adjustments (i.e., inflation).

2. Commercially Reasonable Rates

2.1 Without limiting Section 11, CDIC's Reserved Rights, of the RFSA, where a Supplier submits rates that are considered to be, in CDIC's sole and absolute discretion, commercially unreasonable, CDIC may deem the rates non-compliant and reject the Financial Offer.

3. Non-Resident Suppliers

3.1 Any Supplier who is a non-resident of Canada for tax purposes shall clearly state this fact in its Financial Offer; otherwise, the Supplier shall be deemed to have represented that it is a resident of Canada for tax purposes.

4. Mathematical Errors

In assessing Financial Offers, subject to Section 11, CDIC's Reserved Rights, of the RFSA, any Supplier affected by mathematical errors identified by CDIC may be contacted for clarification.

5. Pricing Tables/Forms

Suppliers submitting under one or more Service Category under Service Stream #1 should provide all applicable rates by fully completing Appendix "D-1" (Financial Offer for Service Stream #1). Suppliers that do not provide Appendix "D-1" will not be qualified for a Service Category under that Service Stream.

[END OF SCHEDULE "D" (FINANCIAL OFFER)]

Appendix "D-1"

Financial Offer for Service Stream #1

In the tables below, the Supplier should provide all-inclusive hourly ceiling rates for the applicable Roles they are qualified to offer for the categories listed for Service Stream #1.

For clarity, the information in the tables will not be evaluated and rates for each Role are not required. However, only SA Holders that have provided a rate for a particular Role may be qualified for that Role under a Service Request.

The following is a list of forty-one (41) Roles for Service Stream #1: Staff Augmentation Services, from the Initial RFSA.

Role #	Service Category #1 - Advisory Services	Level 1	Level 2	Level 3
1	IT Executive Strategic Advisor	$	$	$
2	Data Strategy Advisor	$	$	$

Role #	Service Category #2 - Project Management	Level 1	Level 2	Level 3
3	Project Management Office Lead	$	$	$
4	Project Manager	$	$	$
5	Project Administrator / Coordinator	$	$	$

Role #	Service Category #3 - Cyber security	Level 1	Level 2	Level 3
6	Security Analyst	$	$	$
7	Application Security Administrator	$	$	$
8	IT Security Architect	$	$	$
9	Ethical / White Hat Hacker (or Penetration Tester)	$	$	$
10	Azure Security Architect	$	$	$
11	Azure Security Administrator	$	$	$

Role #	Service Category #4 - Enterprise Technology	Level 1	Level 2	Level 3
12	Storage Administrator / Virtualization Architect	$	$	$
13	Systems Architect (network, data, applications)	$	$	$
14	Azure Architect	$	$	$
15	Azure Administrator	$	$	$
16	Azure Data Base Administrator	$	$	$
17	Webmaster	$	$	$

Role #	Service Category #5 - Technical Support	Level 1	Level 2	Level 3
18	Application Support Specialist	$	$	$
19	Deskside Technical Support Analyst	$	$	$
20	Service Desk Analyst	$	$	$
21	IT Service Management Specialist	$	$	$
22	Security Incident Responder	$	$	$
23	Infrastructure Operations and Support	$	$	$
24	Technical Writer / Trainer / Courseware Author (Developer)	$	$	$

Role #	Service Category #6 – SharePoint Support	Level 1	Level 2	Level 3
25	SharePoint Online Administrator	$	$	$
26	SharePoint Online Architect	$	$	$
27	SharePoint Online Developer	$	$	$

Role #	Service Category #7 – Salesforce Support	Level 1	Level 2	Level 3
28	Salesforce Developer	$	$	$
29	Salesforce Tester	$	$	$
30	Salesforce Administrator	$	$	$

Role #	Service Category #8 – Alteryx Support	Level 1	Level 2	Level 3
31	Alteryx Developer	$	$	$

Role #	Service Category #9 – Agile Application Delivery	Level 1	Level 2	Level 3
32	Scrum Master	$	$	$
33	Agile Team Coach	$	$	$

Role #	Service Category #10 - Application Development	Level 1	Level 2	Level 3
34	Solution Architect	$	$	$
35	Business Analyst	$	$	$
36	Application Developer	$	$	$
37	Azure Cloud Application Developer	$	$	$
38	Quality Assurance (QA)Tester	$	$	$

Role #	Service Category #11 - Business Intelligence and Analytics	Level 1	Level 2	Level 3
39	Business Intelligence Developer	$	$	$
40	Data Architect	$	$	$
41	Data Scientist	$	$	$

The following is a list of eight (8) additional Roles for Service Stream #1: Staff Augmentation Services, applicable to this RFSA 2021 Refresh.

Role #	Service Category #2 - Project Management	Level 1	Level 2	Level 3
42	IT Service Manager	$	$	$

Role #	Service Category #3 - Cyber security	Level 1	Level 2	Level 3
43	Cyber Forensics Specialist	$	$	$
44	Security Engineer (Application/Network)	$	$	$
45	SOC Analyst	$	$	$
46	SOC Lead/Manager	$	$	$
47	Cloud Security Specialist	$	$	$
48	Security Administrator	$	$	$
49	Governance Risk and Compliance Analyst	$	$	$

[END OF APPENDIX "D-1" (FINANCIAL OFFER FOR SERVICE STREAM #1)]

Schedule "E"

Mandatory Proposal Forms

The following is a list of mandatory forms which must be included in the Supplier's Proposal as applicable.

Schedule/Appendix	Proposal Form Required
Schedule "C"	Technical Offer *(One (1) per Proposal)*
Appendix "C-1"	Technical Offer Form (One (1) per *Proposal*)
Appendix "C-2"	Reference Engagement Form *(Three (3) per Service Category)*
Schedule "D"	Financial Offer *(One (1) per Proposal)*
Appendix "D-1"	Financial Offer for Service Stream #1 (One (1) per *Proposal*) *NOTE: This Appendix is **ONLY** required for Suppliers offering a Service Category under Service Stream #1.

[END OF SCHEDULE "E" (MANDATORY PROPOSAL FORMS)]

Schedule "F"

Form of Professional Services Agreement

Substantial changes to the Professional Services Agreement will not be considered. As per Section 14, Resulting Agreements and Term of Agreement, CDIC intends to award agreements based on this Schedule "F" (Form of Professional Services Agreement) to successful Suppliers. As such, any requests for changes to the Professional Services Agreement will only be considered from successful Suppliers.

PROFESSIONAL SERVICES AGREEMENT

THIS AGREEMENT is made as of the Execution Date

BETWEEN:

CANADA DEPOSIT INSURANCE CORPORATION,
a federal crown corporation established by an Act of Parliament

the *Canada Deposit Insurance Corporation Act*
("**CDIC**")

AND:

[insert name of corporation or partnership],
a corporation incorporated under the laws of <*>
or
a (**limited liability**) partnership established pursuant to the laws of <*>
("**Supplier**").

BACKGROUND

A. Following a request-for-supply arrangements process, CDIC has selected the Supplier to provide the Services on a standby/as-needed basis as set out in Appendix A to this Agreement. CDIC makes no guarantee as to the value or volume of work to be assigned to any Supplier, if any, and Supplier acknowledges same.

B. The Supplier is qualified to provide the Services and agrees to provide the Services in accordance with the terms and conditions of this Agreement.

IN CONSIDERATION of the above, the mutual covenants set out herein, and other good and valuable consideration (the receipt and sufficiency of which are hereby acknowledged), the Parties agree as follows:

ARTICLE 1
DEFINITIONS AND INTERPRETATION

1.1 Definitions. Whenever used in this Agreement, the following words and terms shall have the meanings set out below:

"**Acceptance**", "**Accepts**", "**Accepted**" or "**Acceptable**" means the confirmation in writing by the Designated Officer that CDIC is satisfied with the quality of the Services provided;

"**Agreement**" means this Professional Services Agreement and includes the appendices and any schedules attached hereto, as such may be amended from time to time by written agreement of the Parties hereto;

"**Assigned Person**" means any person employed or engaged by the Supplier who is (i) assigned by the Supplier to perform the Services and is listed in Appendix A, or (ii) who is assigned by the Supplier to perform the Services as an alternate, pursuant to Section 6.5;

"**Business Day**" means a day, other than a Saturday, Sunday or a statutory or civic holiday in the City of Ottawa, Province of Ontario, Canada;

"**Claim**" means any claim, demand, action, assessment or reassessment, suit, cause of action, damage, loss, charge, judgment, debt, costs, liability or expense, including taxes, interest and penalties imposed by law and the reasonable professional fees and all costs incurred in investigating or pursuing, defending or settling any of the foregoing or any proceeding relating to any of the foregoing;

"**Commencement Date**" means the date set out in Appendix A on which the Supplier shall begin to provide the Services;

"**Completion Date**" means the date set out in Appendix A on which the Supplier shall cease to provide the Services;

"**Confidential Information**" has the meaning attributed thereto in Appendix C;

"**Designated Officer**" means the individual set out in Appendix A who represents CDIC, or such other person as may be designated by CDIC from time to time;

"**Disbursements**" mean the reasonable fees, expenses, costs or charges, from other parties that are incurred by the Supplier for the purpose of performing the Services including all applicable taxes thereon, but do not include Pre-approved Expenses;

"**Execution Date**" means the latest date this Agreement is signed by the Parties as indicated on the signature page;

"**Fee**" or "**Fees**" means an amount agreed to be paid to the Supplier for the provision of any part of the Services as set out in Appendix A;

"**GST/HST/PST**" means all taxes exigible under Part IX of the *Excise Tax Act*;

"**Information**" means all information provided to the Supplier and any Assigned Person, regardless of form or medium, whether reproducible or not, and includes any facts, data, hypotheses, analyses, projections, assumptions, or opinions;

"**Intellectual Property Rights**" means any rights provided under: (i) patent law; (ii) copyright law (including moral rights); (iii) trade-mark law; (iv) design patent or industrial design law; (v) semi-conductor chip or mask work law; or (vi) any other statutory provision or common law principle applicable to this Agreement, including trade secret law, which may provide a right in either hardware, software, documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how generally, or the expression or use of such hardware, software, documentation, Confidential Information, ideas, formulae,

algorithms, concepts, inventions, processes or know-how; or any rights provided under any applications, registrations, licenses, sub-licenses, franchises, agreements or any other evidence of a right in any of the foregoing;

"**Non-Compliant Jurisdiction**" means any jurisdiction whose laws conflict with or impede the application of the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*, either expressly or through subsequent application. This includes the United States of America;

"**Parties**" means CDIC and the Supplier, and "**Party**" means either one of them;

"**person**" includes an individual, a corporation, a general or limited partnership, a joint venture, a trust, an unincorporated organization, the Crown or a federal, provincial, national, state or municipal government or any agency or instrumentality of the Crown or a government or any entity recognized by law;

"**Personal Information**" means Information about an identifiable individual;

"**Pre-approved Expenses**" mean the reasonable out-of-town travel, accommodation and living expenses, including all applicable taxes thereon, that are expected to be incurred by the Supplier for the purpose of performing the Services and that are approved by CDIC's Designated Officer prior to actually being incurred;

"**Services**" means the tasks or activities required to be performed by the Supplier as set out in Appendix A and any services ancillary thereto;

"**Service Request**" means a document issued by CDIC to a Supplier, that includes instructions and applicable CDIC service requirements, which may result in a Task Authorization;

"**Task Authorization**" means the authorization issued by CDIC, following the receipt of a Supplier's response to a Service Request, authorizing services to commence;

"**Total Fee**" means the total amount payable to the Supplier for the provision of the Services as set out in Appendix A and any services ancillary thereto; and

"**Work Product**" means all materials, inventions and other deliverables that the Supplier may develop for CDIC in the course of providing the Services, whether alone or jointly with others, including all research, reports, correspondence, memoranda, notes, source code, object code, executable code, technical documentation, user documentation, custom software and all information generated by the Supplier specifically for CDIC in any reproducible medium in connection with the provision of the Services.

1.2 Certain Rules of Interpretation. In this Agreement,

(a) **Time** - the Supplier will use all reasonable efforts to complete within any agreed upon time frame the performance of the Services. However, the Supplier will not be liable for failures or delays in performance that arise from causes beyond its control;

(b) **Currency** - unless otherwise specified, all references to monetary amounts in this Agreement are to lawful currency of Canada;

(c) **Headings** - descriptive headings of Articles and Sections are inserted solely for convenience of reference and are not intended as complete or accurate descriptions of the content of such Articles or Sections and as such, shall not affect the construction or interpretation of this Agreement;

(d) **Singular, etc**. - words expressed in the singular include the plural and vice-versa and words in one gender include all genders;

(e) **Consent** - whenever a provision of this Agreement requires an approval or consent by a Party to this Agreement and notification of such approval or consent is not delivered within the applicable time, then, unless otherwise specified, the Party whose consent or approval is required shall be conclusively deemed to have withheld its approval or consent;

(f) **Calculation of Time** - unless otherwise specified, time periods within or following which any payment is to be made or act is to be done shall be calculated by excluding the day on which the period commences and including the day on which the period ends;

(g) **Business Day** - whenever any payment is to be made or action to be taken under this Agreement is required to be made or taken on a day other than a Business Day, such payment shall be made or action taken on the next Business Day following such day;

(h) **Inclusion** - where the words "including" or "includes" appear in this Agreement, they mean "including without limitation" or "includes without limitation" respectively;

(i) **References** - the words "herein", "hereof", "hereby" and "hereunder" and similar expressions refer to this Agreement as a whole and not to any particular portion of it and references to an Article, Section or subsection refer to the applicable Article, Section or subsection of this Agreement; and

(j) **No Strict Construction** – the language used in this Agreement is the language chosen to express the mutual intent of the Parties, and no rule of strict construction will be applied against either of the Parties.

1.3 **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein. The rights and obligations under this Agreement shall not be governed by the *United Nations Convention on Contracts for the International Sale of Goods* or any local implementing legislation, the application of which is expressly excluded.

1.4 **Appendices**. The appendices to this Agreement listed below include additional terms which form part of this Agreement:

Appendix	**Description**
A	Services and Fees
B	Service Categories/Roles
C	Confidentiality, Privacy, Conflict of Interest and Security
D	Service Request Form

ARTICLE 2
AGREEMENT FOR SERVICE

2.1 The Supplier is hereby engaged by CDIC as of the Execution Date as an independent contractor on a non-exclusive basis for the sole purpose of undertaking and delivering the Services set out in Appendix A, any Task Authorization, and any applicable Work Product for the term set out therein, and in accordance with this Agreement.

2.2 Subject to the conflict of interest provisions contained in Appendix C, CDIC acknowledges that, during the term of this Agreement, the Supplier and any Assigned Person may provide services to other persons (including member institutions of CDIC or any parent or subsidiary corporations or affiliates thereof).

2.3 The Supplier is responsible for the delivery of all filings required in relation to, and the payment of: all taxes, levies, premiums or payments assessed, levied or charged against the Supplier, including any GST/HST/PST, income tax, local tax, workplace safety and insurance premiums, Canada Pension Plan or Quebec Pension Plan premiums, Employment Insurance premiums and Ontario Health Insurance Plan premiums or levies or other contributions as required by all laws applicable to the Supplier or to any Assigned Person (all collectively, the "**filings and deductions**"). In addition to any other indemnifications contained in this Agreement, the Supplier agrees to indemnify and save harmless CDIC, its employees, agents, officers and directors from any Claims arising as a result of or in relation to:

(a) the Supplier's failure, omission or refusal to deliver or remit any filings and deductions to the appropriate federal, provincial or municipal government entity, agency or collecting body, as required by law; or,

(b) a determination by any federal, provincial or municipal government entity, agency or collecting body that (notwithstanding the express and mutual intention of the Parties,) the relationship between CDIC and any of the Supplier or any Assigned Person, is not an independent contractor relationship.

ARTICLE 3
LIMITATION OF AUTHORITY

3.1 The Supplier shall have no authority to enter into any contract, commitment or obligation of any kind whatsoever on behalf of CDIC unless the Supplier receives prior written authorization from CDIC.

3.2 Neither the Supplier nor any Assigned Person shall, at any time, be deemed to be an employee, servant or agent of CDIC or of Her Majesty in Right of Canada, for any purpose whatsoever.

ARTICLE 4
CONFIDENTIALITY AND CONFLICT OF INTEREST AND USE OF PERSONAL AND CONFIDENTIAL INFORMATION

4.1 The Supplier agrees to be bound by the terms set out in this Article 4 and in the attached Appendix C entitled "Confidentiality, Privacy Conflict of Interest and Security".

4.2 The Supplier agrees that prior to allowing any Assigned Person to perform the Services, it shall require that Assigned Person to read and agree to abide by the terms of the attached Appendix C entitled "Confidentiality, Privacy, Conflict of Interest and Security".

4.3 Except as set out in Appendix A, the Supplier represents and warrants that:

(a) The Supplier only carries on business in Canada;

(b) The Supplier does not have a parent, subsidiary or other related company that operates in a Non-Compliant Jurisdiction;

(c) The Supplier does not subcontract or outsource data processing or storage to any third party carrying on business in a Non-Compliant Jurisdiction; and

(d) The Supplier's employees are bound by written confidentiality agreements or binding confidentiality policies.

4.4 The Supplier agrees that:

(a) CDIC shall retain custody and control of any Confidential Information and Personal Information transferred, collected, created, obtained, maintained or otherwise held by the Supplier for the purposes of this Agreement, and all Confidential Information and Personal Information must be returned to CDIC upon request;

(b) Except as set out in Appendix A, the Supplier shall not transfer Personal Information to any entity or person carrying on business in a Non-Compliant Jurisdiction for any purpose unless approved by CDIC in writing. Confidential Information may be disclosed to third parties that provide data processing, storage and similar services to the Supplier and may correspondingly be used, processed and stored outside Canada by the Supplier and such third-party service providers. The Supplier is responsible to CDIC for causing such third-party service providers to comply with the obligations of confidentiality set out in this Agreement;

(c) CDIC shall have the right to review from time to time the measures and practices adopted by the Supplier to perform its obligations under this Agreement. This right of review includes the right to be escorted, in accordance with the Supplier's security rules and heavily restricted to certain areas of the Supplier's premises on reasonable written notice to the Supplier to attend the Supplier's premises on reasonable written notice to the Supplier to review such measures and practices and the right to audit the Supplier's relevant records and otherwise verify audit trails for data access, modification or disclosure. The Supplier shall provide full cooperation in connection with any such review. To the extent that such review causes the Supplier to incur reasonable third-party expenses, such expenses shall be reimbursed by CDIC;

(d) The Supplier shall implement sufficient audit trail requirements to record access to Confidential Information and any attempted access thereto and any modification or disclosure of Confidential Information; and

(e) The Supplier shall include the above representations, warranties and terms in any agreement with a third party respecting the transfer of Confidential Information or Personal Information, *mutatis mutandis*.

4.5 If the Supplier learns of any actual or reasonably suspected access, use, destruction, alteration or disclosure of Confidential Information or Personal Information that is not permitted by this Agreement or otherwise approved by CDIC in writing (including any loss or theft of Confidential Information or Personal Information) (collectively, a "**Data Breach**"), Supplier shall promptly notify CDIC in writing of the particulars of such Data Breach (unless such notice is prohibited by applicable law). The Supplier shall thereafter contain and investigate the Data Breach and fully cooperate with CDIC in resolving the Data Breach.

4.6 In the event of a change in status or ownership of a parent company or of the Supplier that may result in a change of custody or control of data being held and/or processed by the Supplier, the Supplier shall promptly notify CDIC. Following such notification, CDIC reserves the right to immediately terminate this Agreement or seek amendments thereto.

4.7 In the event of a change in the operations of the Supplier, such as acquiring or creating an entity in a Non-Compliant Jurisdiction that shall have access to CDIC Information, the Supplier shall promptly notify CDIC. Following such notification, CDIC reserves the right to immediately terminate this Agreement or seek amendments thereto.

ARTICLE 5
CDIC'S RESPONSIBILITIES

5.1 If and when necessary, CDIC shall provide the Supplier with limited access, as required, to its offices and personnel at 50 O'Connor Street, Ottawa, Ontario and 79 Wellington Street West, Suite 1200, Toronto, Ontario (collectively, the "**Premises**") to facilitate the provision of the Services. The Supplier agrees to abide by the requirements of CDIC and the Designated Officer with respect to security, timing and manner and method of access, occupancy and egress from the Premises, as those requirements may change from time to time. The Supplier further agrees to abide by any rules regarding access, occupancy and egress imposed by the landlord of the Premises.

5.2 The Designated Officer, or other representative of CDIC, as may be appropriate, shall provide the Supplier with the Information and Confidential Information that is required for the provision of the Services.

5.3 CDIC acknowledges that the provision of the Services may require the Designated Officer and other CDIC personnel to be available for meetings with the Supplier and to respond promptly to the inquiries of the Supplier. CDIC shall use reasonable efforts to accommodate same without disrupting its operations.

5.4 The Supplier shall consult with the Designated Officer from time to time, regarding the provision of the Services. The Designated Officer may provide the Supplier with a schedule for the completion of the Services (the "**Schedule**").

5.5 CDIC may, at its own discretion, periodically or from time to time, advise the Supplier as to whether the provision of Services by the Supplier is Acceptable. CDIC shall have the right to require the Supplier to correct or replace any Services and Work Product that are deemed by CDIC not to be Acceptable, at the Supplier's own expense. CDIC shall inform the Supplier of the reasons for any such non-Acceptance of the Services or Work Product as the case may be.

5.6 CDIC or its representatives may, at any time during the term of this Agreement or within one (1) year of the expiration or termination of this Agreement, upon reasonable prior written notice to Supplier, and during the regular business hours of the Supplier conduct an audit of the books, accounts, records, and data of the Supplier relating to the performance of the Services and of all expenditures or commitments made by the Supplier in connection therewith. The Supplier shall not, without the prior written consent of CDIC, dispose of any books, accounts or records that relate to the performance of the Services until the later of: (i) the expiration of one (1) year after the final payment is made under this Agreement; or (ii) the settlement of all outstanding claims and disputes between the Parties. The Supplier shall provide CDIC with access to all books, accounts, and records related to the performance of the Services and shall reasonably co-operate with CDIC in respect of any audit that is conducted.

ARTICLE 6
SUPPLIER'S RESPONSIBILITIES

6.1 The Supplier represents and warrants that it is validly incorporated under the laws of <*> and that it has the power and authority to enter into this Agreement. The Supplier represents and warrants that the Supplier and each Assigned Person has the necessary resources, competence and qualifications, including knowledge, skill and experience to provide the Services. The Supplier shall provide the Services promptly, efficiently, in accordance with reasonable standards of quality acceptable to CDIC, in consultation with the Designated Officer, in conformity with the Schedule established by the Designated Officer, if any, and with the terms and provisions of this Agreement.

6.2 The Supplier shall commence the provision of the Services on the Commencement Date and shall provide the Services until the earlier of the Completion Date or the date on which the Services are completed by the Supplier and Accepted by the Designated Officer.

6.3 The Supplier shall make periodic written reports, as requested by the Designated Officer, outlining the progress made by the Supplier in providing the Services.

6.4 CDIC is required to notify individuals in connection with the collection of Personal Information by CDIC. The Supplier agrees that prior to providing any Personal Information about an Assigned Person to CDIC, or prior to allowing an Assigned Person to perform the Services, as applicable, the Supplier shall either (a) provide the Assigned Person with CDIC's privacy notice (a copy of which is at *http://www.cdic.ca/en/about-cdic/policies-*

reports/atip/Pages/Privacy.aspx), or (b) refer the Assigned Person to the webpage where the privacy notice is posted, and require the Assigned Person to read the privacy notice.

6.5 The Supplier shall ensure that the Services are only provided by the Assigned Persons listed in Appendix A hereof and that such Assigned Persons are available to perform the Services in accordance with the Schedule established by the Designated Officer, if any. Should such Assigned Person be unavailable to provide the Services, the Supplier may, with CDIC's prior written consent, acting reasonably, assign an alternate Assigned Person who has a comparable level of skill, ability and qualifications to provide the Services. Other amendments to the list of Assigned Persons in Appendix A may be made with the written consent of CDIC.

6.6 CDIC shall have access at all reasonable times to the books, accounts, records, data, Work Product and other information in the Supplier's and any Assigned Person's possession and control in connection with the provision of the Services.

6.7 On termination for any reason other than breach by CDIC, to the extent that it may exist, in whole or in part, the Supplier shall deliver to CDIC, or such person as CDIC may designate, the Work Product and knowledge that is required by CDIC to complete the provision of the Services or that will allow CDIC to utilize the Services or Work Product on an ongoing basis.

6.8 The Supplier warrants that no Work Product will infringe or otherwise violate any Intellectual Property Rights of any third party.

6.9 The Supplier warrants that all Services and Work Product provided under this Agreement will, at the time of Acceptance, be free from any defect in workmanship and conform to the requirements of this Agreement. If the Supplier is required to correct or replace the Services or Work Product or any portion thereof, it shall be at no cost to CDIC, and any Services or Work Product corrected or replaced by the Supplier shall be subject to all the provisions of this Agreement to the same extent as the Services or Work Product as initially performed.

6.10 The Supplier acknowledges and agrees that it shall, and that CDIC may require the Supplier to require any Assigned Person, to act in conformity with any existing or future policies, standards, guidelines and procedures of CDIC as may become appropriate in CDIC's discretion, at all times during the provision of the Services, including:

a) where the Services involve Personal Information or other "Protected Information", as that term is defined in CDIC's *Information Classification Standard*, the Supplier will adhere to CDIC's *Corporate Security Policy;*

b) where the Services involve travel and related living expenses, the Supplier will adhere to CDIC's *Travel, Hospitality, Conferences and Events Policy*; and

c) where any Assigned Person will be performing Services at CDIC's Premises on a regular basis, to require any Assigned Person to review and act in conformity with: (i) the Guidelines for Contractor/Suppliers' Personnel/Agency Personnel (the "**Guidelines**") and (ii) *Harassment and Violence Prevention Policy* prior to or on the date such Assigned Person commences performing the Services; and (iii) CDIC's *Vaccination Policy for Third-Parties*.

6.11 The Supplier shall be responsible for ensuring that each Assigned Person complies with all of the terms of this Agreement and shall be responsible for any non-compliance in any way attributable to any Assigned Person or other person for whom the Supplier is responsible.

ARTICLE 7
OWNERSHIP OF INTELLECTUAL PROPERTY

7.1 The Supplier agrees that prior to allowing any Assigned Person to perform the Services, it shall require that Assigned Person to read and agree to abide by the terms of this Article 7.

7.2 If, during the course of providing Services to CDIC, the Supplier develops any work for CDIC that is protected by copyright, the Supplier hereby waives unconditionally any moral rights it may have in such work and shall require each Assigned Person to waive unconditionally any moral rights in such work upon applicable payment by CDIC to Supplier.

7.3 The Supplier shall not use or disclose any Work Product or other materials embodying any of CDIC's Intellectual Property Rights provided by CDIC or developed for CDIC except in the course of providing the Services or as expressly authorized by CDIC in writing.

7.4 The Supplier shall not make any unauthorized use of any trade secrets or Intellectual Property Rights of a third party during the course of providing Services to CDIC.

7.5 The Supplier shall not make any unauthorized use of CDIC's property including its computer systems, communications networks, databases or files, and shall adhere to all CDIC policies regarding the use of such computer systems, communication networks, databases or files provided that such policies have been provided to Supplier in writing prior to execution of this Agreement.

7.6 The Supplier shall only use software authorized by CDIC on CDIC equipment.

7.7 The Supplier acknowledges and agrees that it shall be held liable for any breach or any damages resulting from any violations of the terms of this Article 7 that are caused by the Supplier or that are attributable in any way to an Assigned Person.

7.8 All Work Product first created for CDIC shall be the exclusive property of CDIC and the Supplier shall have no right, title or interest in any such Intellectual Property Rights. At the request and expense of CDIC, the Supplier shall do all acts necessary and sign all documentation necessary in order to assign all rights in the Intellectual Property Rights to CDIC and to enable CDIC to register patents, copyrights, trade-marks, mask works, industrial designs and such other protections as CDIC deems advisable anywhere in the world.

7.9 The Supplier agrees to provide all reasonable assistance to CDIC in the prosecution of any patent application, copyright registration or trade-mark application or the protection of any Intellectual Property Rights. The Supplier agrees to execute any documentation necessary to assist with any such prosecution or to effect any such application or registration upon the request of CDIC, whether such request is made during the term of this Agreement or after the expiration or termination of this Agreement for any reason whatsoever.

ARTICLE 8
FEES AND BILLING PROCEDURES

8.1 The Total Fee payable under this Agreement is as set out in Appendix A. The Supplier shall have no right to demand any additional Fees other than as set out in Appendix A, either before, during or after the completion of provision of the Services.

8.2 In accordance with the terms of Appendix A, the Supplier shall deliver a written request for payment in the form of an invoice for services rendered to CDIC (the "**Invoice**").

8.3 The Invoice shall be accompanied by supporting documentation confirming the amount and particulars of any Disbursements or Pre-approved Expenses incurred by the Supplier in providing the Services and shall specify the following information, as applicable:

(a) a detailed suitable description of the Services provided in relation to the Fees billed by the Supplier;

(b) the amount owing in accordance with the Fees set out in Appendix A;

(c) the amount of GST/HST/PST thereon;

(d) the amount of any Disbursements and Pre-approved Expenses; and

(e) such other information as CDIC may reasonably require.

The Supplier agrees that failure to include all supporting documentation with the Invoice and/or failure to provide any or all of the foregoing information as part of the Invoice may result in a delay of payment to the Supplier.

8.4 Within thirty (30) days of receiving an Invoice, CDIC shall verify the amounts stipulated in the Invoice and subject to Section 8.1 hereof, shall pay to the Supplier the full amount of the Invoice. CDIC shall advise the Supplier of the details of any objection it may have to the form, content or amount of the Invoice within fifteen (15) days of receipt of the Invoice, and the above-noted thirty (30) day period shall commence to run after receipt by CDIC of a revised Invoice.

8.5 Subject to Section 9.3 hereof, upon termination of this Agreement by CDIC, the Supplier shall, within fifteen (15) days after the effective date of such termination, deliver a final Invoice to CDIC in the form specified above setting out the Fees, GST/HST/PST, Disbursements, and Pre-approved Expenses charged or incurred by the Supplier from the date of the previous Invoice to the effective date of termination and CDIC shall pay the Invoice in accordance with this Article 8. The Supplier shall not be entitled to payment for any amount on account of Fees, GST/HST/PST, Disbursements or Pre-approved Expenses that are either charged or incurred by the Supplier following the effective date of termination of this Agreement.

ARTICLE 9
EXPIRATION AND TERMINATION

9.1 CDIC may terminate this Agreement at any time by giving the Supplier ten (10) business days prior written notice. The Supplier and CDIC agree and acknowledge that the giving of such written notice shall serve to discharge all liability whether contractual, statutory, or otherwise owed by CDIC to the Supplier, except CDIC's obligation to pay the Supplier any outstanding Fees earned and GST/HST/PST thereon, and any Disbursements or Pre-approved Expenses incurred by the Supplier in the period prior to the effective date of termination of this Agreement which obligation shall survive such termination.

9.2 If the Supplier breaches any provision of this Agreement and fails to remedy such breach within five (5) Business Days of receiving a written notice from CDIC notifying the Supplier of such breach, CDIC may, without giving any further notice to the Supplier, terminate this Agreement effective as of the end of such five (5) day period.

9.3 Notwithstanding any other provision of this Agreement, if this Agreement is terminated by CDIC pursuant to Section 9.2 above:

(a) the Supplier shall not be entitled to payment for any amount on account of Fees, GST/HST/PST, Disbursements or Pre-approved Expenses that are charged or incurred by the Supplier after the day upon which such notice of breach of the Agreement is received by the Supplier; and,

(b) CDIC may arrange, upon such terms and conditions and in such manner as CDIC deems appropriate, for any uncompleted Services to be completed and the Supplier shall be liable to CDIC for any amounts in excess of the Total Fee as are required to retain a replacement Supplier to complete the Services. CDIC may, in its sole discretion, withhold from the amount due to the Supplier upon termination of this Agreement such sums as CDIC determines to be necessary to protect CDIC against any excess costs it might incur in relation to the retention of a replacement Supplier and the completion of the Services.

9.4 If the Services are not provided in full, the Supplier shall be entitled to payment of that portion of the Total Fee represented by the Services performed as determined by CDIC acting reasonably and based on the agreed upon scope of Services.

9.5 This Agreement shall expire automatically on the earlier of the Completion Date or the date on which the Services are completed by the Supplier and Accepted by the Designated Officer.

9.6 Upon expiration or termination of this Agreement for any reason whatsoever, the Supplier shall forthwith return all Information, Confidential Information, Work Product and other materials embodying CDIC's Intellectual Property Rights in the possession or control of the Supplier or any Assigned Person to CDIC or shall provide a written certificate to CDIC certifying the destruction of all Information, Confidential Information, Work Product and other materials embodying CDIC's Intellectual Property Rights if instructed by CDIC to destroy such Information.

ARTICLE 10
INDEMNIFICATION

10.1 CDIC agrees to indemnify, defend and hold harmless the Supplier and its respective employees, agents, officers, directors, successors and assigns (each, a "**Supplier Indemnitee**"), from and against any Claims that may be made or brought against the Supplier Indemnitee, or which they may suffer or incur, directly as a result of any deliberate or negligent acts or omissions by CDIC or any person for whom CDIC is responsible.

10.2 The Supplier agrees to indemnify, defend and hold harmless CDIC and its respective employees, agents, officers, directors, successors and assigns (each, a "**CDIC Indemnitee**") from and against any Claims that may be made or brought against the CDIC Indemnitee, or which they may suffer or incur, directly or indirectly as a result of or in connection with:

(a) any deliberate or negligent acts or omissions of the Supplier or any person for whom the Supplier is responsible (including any Assigned Person);

(b) any injury sustained by the Supplier or by any Assigned Person while on the Premises for any reason connected with this Agreement;

(c) the infringement, alleged infringement or potential infringement by any aspect of the Services or the Work Product of the Intellectual Property Rights of any person;

(d) any breach by the Supplier or any Assigned Person of Article 4 or the obligations to protect Confidential Information or Personal Information; or

(e) any other breach of this Agreement by the Supplier or by any Assigned Person.

10.3 The obligation to indemnify in respect of any Claim is contingent upon the CDIC Indemnitee or the Supplier Indemnitee (as applicable) (the "**Indemnified Party**") (a) giving prompt written notice thereof to the indemnifying Party (the "**Indemnifying Party**") and (b) providing reasonable co-operation and assistance to the Indemnifying Party in the investigation, defence, negotiation and settlement of any Claim, including providing reasonable access to relevant information and employees. The obligation to indemnify in respect of any Claim shall terminate unless the Indemnified Party gives the aforementioned written notice to the Indemnifying Party within two (2) years of the date on which the Indemnified Party knew or ought reasonably to have known of the existence of the Claim.

10.4 **Third Party Claims**. In respect of any third party Claim, the Indemnifying Party will be entitled to elect by written notice addressed to the Indemnified Party, within fifteen (15) days after its receipt of such notice, to assume control over the investigation, defence, negotiation and settlement of such third party Claim at its own cost, risk and expense.

(a) If the Indemnifying Party elects to assume such control, the Indemnified Party will have the right to participate in the investigation, defence, negotiation and settlement of such third party claim at the cost of the Indemnifying Party and to retain counsel

to act on its behalf, provided that the fees and disbursements of such counsel will be paid by the Indemnified Party unless the Indemnifying Party consents to the retention of such counsel or unless the named parties to any action or proceeding include both the Indemnifying Party and the Indemnified Party and the representation of both the Indemnifying Party and the Indemnified Party by the same counsel would be inappropriate due to the actual or reasonably potential differing interests between them (such as the availability of different defences). The Indemnifying Party will not settle any Claim without the prior written consent of the Indemnified Party.

(b) If the Indemnifying Party does not elect to assume control of the investigation, defence, negotiation and settlement of the third party Claim, or if the Indemnifying Party, having elected to assume such control thereafter fails to diligently defend the third party Claim, the Indemnified Party will have the right to assume such control in such reasonable manner as it may deem appropriate, at the cost, risk and expense of the Indemnifying Party, and the Indemnifying Party will be bound by the results obtained by the Indemnified Party with respect to such third party Claim. The Indemnifying Party will have the right to participate in such defence at its own cost and expense.

10.5 **Set-off and Subrogation**. The indemnity obligations hereunder will be enforceable without right of set-off, counterclaim or defence as against the Indemnified Party. The Indemnifying Party will, upon payment of an indemnity in full under this Agreement, be subrogated to all rights of the Indemnified Party with respect to the claims and defences to which such indemnification relates.

ARTICLE 11
DISPUTE RESOLUTION

11.1 Subject to Section 11.4 below, all matters to be decided or agreed upon by the Parties under this Agreement and all disputes which may arise with respect to any matter governed by this Agreement shall at first instance be decided or resolved by the most senior Assigned Person or Designated Officer of each Party. Each Party acknowledges that it is in their mutual best interests to make all such decisions by mutual agreement and agrees to act reasonably and in good faith in order to permit and encourage their employees and officers to do so.

11.2 If the Assigned Person or Designated Officer noted above are not able to resolve any dispute referred to them within fifteen (15) days of such referral, or if they are not able to agree on any other matter required to be decided by them under this Agreement, either Party may refer the matter to arbitration in accordance with the provisions of the *Commercial Arbitration Act*, R.S.C., 1985, c. 17 (2nd Supp.).

11.3 No Party may bring legal proceedings in respect of any issue that is to be submitted to arbitration hereunder unless that Party has complied with subsection 11.1 and 11.2.

11.4 Notwithstanding the above, each Party reserves the right to seek equitable relief in a court of competent jurisdiction to protect Intellectual Property Rights, Confidential Information or Personal Information.

ARTICLE 12
SURVIVAL OF TERMS OF AGREEMENT

12.1 All of:

(a) the Supplier's and any Assigned Person's obligations regarding confidentiality of information and ownership of Intellectual Property Rights under Articles 4 and 7 and Appendix C;

(b) the provisions regarding indemnification; and

(c) the provisions regarding dispute resolution,

shall survive the expiration or termination of this Agreement for any reason whatsoever, as shall any other provision of this Agreement which, by the nature of the rights or obligations set out therein, might reasonably be expected to so survive.

ARTICLE 13
GENERAL

13.1 **Entire Agreement**. This Agreement constitutes the entire agreement between the Parties pertaining to the subject matter of this Agreement and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, of the Parties pertaining to that subject matter. No supplement, modification or waiver or termination of this Agreement shall be binding unless executed in writing by the Party to be bound thereby.

13.2 **Amendments**. This Agreement may be changed, amended or modified at any time by written instrument executed by the authorized representatives of the Parties, except for amendments to the list of Assigned Persons in Appendix A pursuant to Section 6.5 which only require the written consent of CDIC.

13.3 **Renewal**. The term of this Agreement may be extended prior to the expiration hereof or this Agreement may be renewed for such period and on such terms and conditions as may be agreed upon in writing by the Parties.

13.4 **Waiver**. No term or provision of this Agreement shall be deemed waived and no breach thereof shall be deemed excused unless such waiver or consent is in writing and signed by the Party waiving or consenting. No waiver or consent by any Party, whether express or implied, shall constitute a waiver or consent for any other term or provision or subsequent breach of such term or provision.

13.5 **Assignment**. Neither this Agreement nor any part of, nor any right, title or interest under this Agreement shall be assigned, sub-contracted or otherwise transferred by the Supplier without CDIC's prior written consent, which consent may be withheld without reason. This Agreement shall enure to the benefit of and bind the Supplier and its successors and permitted assigns.

13.6 **Publicity**. The Supplier shall not refer to this Agreement, nor to any of its rights or obligations under this Agreement, in any public forum, or for the purpose of promoting itself or its products or services, without the prior written consent of CDIC. The Supplier acknowledges that CDIC is subject to the *Access to Information Act* and, as a consequence, CDIC may be required to disclose any information contained in this Agreement including, but not limited to, the name of the Supplier and/or any Assigned Person, the Total Fee, the description of the Services and any Work Product arising therefrom. The Supplier also acknowledges that CDIC may refer to any information contained in this Agreement on its website.

13.7 **No Solicitation**. The Parties agree that, unless otherwise agreed to by the Parties in writing, during the term of this Agreement neither Party shall directly or indirectly solicit as an employee or independent contractor an employee of or Supplier to the other Party or a former employee of or Supplier to the other Party that is or was involved in providing the Services under this Agreement.

13.8 **Severability**. If any of the provisions contained in this Agreement are found by a court of competent jurisdiction to be invalid, illegal or unenforceable in any respect, the validity, legality or enforceability of the remaining provisions contained herein shall not in any way be affected or impaired thereby.

13.9 **Further Assurances**. The Parties hereto agree, from time to time after the execution of this Agreement, to make, do, execute or cause or permit to be made, done or executed all such further and other lawful acts, deeds, things, devices, conveyances and assurances in law whatsoever as may be required to carry out the true intention and to give full force and effect to this Agreement.

13.10 **Enforceability**. Each Party affirms that it has full power and authority to enter into and perform the terms of this Agreement, and that the person(s) signing this Agreement on behalf of each Party is (are) properly authorized and empowered to sign it. Each Party further acknowledges that prior to execution of this Agreement, it has read this Agreement, has had the opportunity to be advised by an independent legal advisor if it so desired, and that it understands and agrees to be bound by this Agreement.

13.11 **Conflict**. In the event of any conflict or inconsistency between this Agreement and the appendices to this Agreement, the terms and conditions set out in this Agreement shall prevail.

13.12 **Remedies**. The remedies expressly stated in this Agreement shall be cumulative and in addition to and not in substitution for those generally available at law or in equity.

13.13 Notices. Any notice required or permitted to be given hereunder in writing may be delivered (including by commercial courier) or sent by facsimile, email or other electronic transmission. Delivered notices shall be deemed received upon delivery during business hours. Notices sent by facsimile, email or other electronic transmission or delivered outside of business hours shall be deemed received on the next Business Day following the day of transmission or delivery. The addresses to be used for any deliveries or transmissions may be changed by notice given in accordance with this Section and, until so changed, shall be as follows:

if to the Supplier:

<*name + address*>

Attention: <*name*>, <*title*>

Fax: <*>
Telephone: <*>
Email: <*>

and if to CDIC:

Canada Deposit Insurance Corporation
50 O'Connor Street, 17th Floor
Ottawa, ON K1P 6L2

Attention: <*name*>, <*title*>

Fax: (613) <*>
Telephone: (613) <*>
Email: <*>@cdic.ca

13.14 Counterparts. This Agreement may be executed in any number of counterparts. Either Party may send a copy of its executed counterpart to the other Party by facsimile, email or other electronic transmission instead of delivering a signed original of that counterpart. Each executed counterpart (including each copy sent by other means) will be deemed to be an original; all executed counterparts taken together will constitute one agreement.

THE PARTIES HAVE EXECUTED this Agreement as of the latest date this Agreement is signed by all the Parties (Execution Date).

CANADA DEPOSIT INSURANCE CORPORATION

Name: <*>
Title: <*>

Date:

I have authority to bind the above corporation.

[Supplier's Name in Caps]

Name: **[Supplier's Representative's Name]**
Title: <*>

Date:

I have authority to bind the above corporation.

Appendix A
SERVICES AND FEES

1. Description of Services

The Supplier agrees to provide to CDIC certain services (the "**Services**") in respect of the Service Stream(s), Service Categories and/or Roles for which the Supplier has qualified, as outlined in Appendix B and the Supplier's Proposal (the "**Proposal**") dated, 2022 submitted in response to this RFSA 2021 Refresh.

In the event of any conflict or inconsistency between (i) this Appendix A and Articles 1 through 13 of the Agreement; and (ii) the attached Proposal, the terms and conditions of this Appendix A and of Articles 1 through 13 shall prevail.

2. Service Request Process

CDIC may issue a written Service Request to the Supplier and to other suppliers selected pursuant to the Request for Supply Arrangement 2020-2842 ("Initial RFSA") and subsequent RFSA Refresh 2021, setting out a brief description of the Services and deliverables required, the timeframes, and any other requirements.

If the Supplier wishes to respond to a Service Request, the Supplier shall prepare, at no cost to CDIC, a written response delivered to CDIC setting out: the list and description of the deliverables; the names and resumes of the resources that the Supplier proposes to assign to each of the Roles (if applicable); the estimated duration for each resource required to achieve completion of the proposed Services within the timeframe specified in the Service Request; the proposed fees (including a detailed breakdown of the fees for particular Services and/or deliverables); and the applicable milestones. The Supplier's response to the Service Request shall comply with the requirements set out in the Service Request. The Supplier shall ensure that each individual proposed is qualified for the Role. The Supplier shall provide CDIC or its representatives with the opportunity to interview its proposed resource(s), at no cost.

If the Supplier receives a Service Request but does not intend to submit a response, the Supplier shall notify CDIC that it will not respond.

CDIC reserves the right to require the SA Holder to replace any deployed resource(s) should an individual not meet CDIC's qualification requirements and performance expectations.

3. Task Authorization

Upon CDIC's acceptance of a Supplier's satisfactory response to the requirements set out in the Service Request, both parties must provide approval in writing, resulting in a Task Authorization, which authorizes Services to commence.

CDIC will issue an amendment to the Task Authorization in the event of any changes to the scope of the Services, activities to be performed, or changes in any schedules that may

be necessary or desirable in light of additional information or actual experience obtained prior to, or in the course of the Services, or as CDIC redefines its needs.

CDIC will not pay the Supplier for any design changes, modifications or interpretations of the Services unless they have been approved, in writing, and CDIC has issued a Task Authorization amendment authorizing the increased expenditure to be incorporated into the work.

CDIC may terminate all or any part of an authorized Task Authorization for the convenience of CDIC on ten (10) days written notice to the Supplier. In the event of such termination, the Supplier agrees that it will be entitled to be compensated only for work performed and accepted up to the effective date of such termination.

CDIC may terminate all or any part of an authorized Task Authorization due to the default of the Supplier at any time on ten (10) day's written notice to the Supplier provided the Supplier has not rectified the default during the notice period. In the event of such termination, the Supplier and CDIC agree that the rights and obligations of the Supplier and CDIC will be governed by the provisions of Article 9. Expiry and Termination of the Agreement.

4. Term

Subject to any earlier termination by CDIC pursuant to the Agreement, the term of this Agreement shall be:

Commencement Date: [Execution Date][or *insert date (if obligations to commence prior to or after the Execution Date)*].
Completion Date: <*>.

The term of this Agreement may be renewed or extended for up to two (2) consecutive one (1) year periods (each, a "**Renewal**") to a maximum of four (4) years, at CDIC's sole option and discretion

5. Fees

The Supplier agrees to provide the Services at the rates (the "**Fees**") set out in Appendix B.

6. Payment Scheduling

The Supplier shall provide an Invoice to CDIC upon completion and Acceptance of the Services.

7. CDIC Designated Officer

Name: <*>
Title: <*>

8. Disclosure Regarding Non-Compliant Jurisdictions

[Insert "None" or describe any disclosures re: Article 4 of the Agreement, if any]

Appendix B
SERVICE CATEGORIES/ROLES

For a description of "Service Categories" and "Roles", refer to RFSA.

[**Instructions: Insert chart for particular Service Categories and/or Roles.]**

Appendix C
CONFIDENTIALITY, PRIVACY, CONFLICT OF INTEREST AND SECURITY

Any capitalized terms used herein but not defined have the meaning set out in the Agreement.

Confidentiality:

1. "**Confidential Information**" means

   (a) any and all technical and non-technical information including patents, copyrights, trade secrets, proprietary information, techniques, sketches, drawings, models, inventions, know-how, processes, apparatus, equipment, algorithms, software programs, software source documents, and formulae related to existing, proposed and future products and services;

   (b) information concerning research, experiments, procurement requirements, manufacturing, customer lists, business forecasts, sales, merchandising and marketing plans;

   (c) proprietary or confidential information of any third party that may rightfully be disclosed by CDIC to the Supplier;

   (d) information which is expressly communicated as being or is marked as confidential;

   (e) information which by its nature and the context in which it is disclosed is confidential;

   (f) all information regarding CDIC or any of its business affairs, liabilities, assets, plans or prospects, including any and all information in respect to the Services and the provision of those Services;

   (g) all information regarding any member or former member institution of CDIC, any parent or subsidiary corporation or affiliate thereof, or any of the business affairs, liabilities, assets, plans or prospects of any member or former member institution of CDIC or any parent or subsidiary corporation or affiliate thereof, disclosed to or received by the Supplier during or as a result of providing the Services, whether originating from CDIC or any other source; and

   (h) all Work Product.

2. The Supplier shall not disclose any Confidential Information, unless such disclosure:

   a. is compelled:

      i. by law in connection with proceedings before a court, commission of inquiry or other public tribunal of competent jurisdiction;

      ii. by law at the request of any regulatory or supervisory authority having jurisdiction; or

      iii. in accordance with the practices and procedures of Parliament (including any committee of the House of Commons or Senate of Canada);

b. is of information that is in the public domain or has come into the public domain other than by reason of a breach of this Appendix (and, for the purpose hereof, information is not considered to be in the public domain merely because it appears in a court file or other repository to which members of the public are capable of having access, but only if it has actually been disseminated to the general public, such as through the news media or the publication of annual or other reports);

c. is of information that has been, or is hereafter, received by the Supplier or any Assigned Person other than from or at the request of CDIC and other than during or as a result of providing the Services;

d. is part of the performance of any part of the Services which is to be done on a shared, cooperative or joint basis with such other persons at the request, or with the concurrence of the Designated Officer who have signed an agreement similar in form and substance to this Appendix; or

e. is made with the prior written consent of the Designated Officer.

3. If the Supplier believes that disclosure of Confidential Information is or is about to be required in one of the circumstances described in subsection 2.a, or in any circumstances not referred to in Section 2, it shall notify CDIC orally as soon as reasonably possible and as much in advance of the impending disclosure as possible, of the circumstances and scope of the disclosure and shall immediately confirm such oral notice in writing.

4. The Supplier agrees that it acquires no right, title or interest to any Confidential Information, except a limited right to use the Confidential Information in connection with the provision of the Services. All Confidential Information remains the property of CDIC or its members and no licence or other right, title or interest in the Confidential Information is granted hereby.

5. The Supplier agrees to protect the Confidential Information and prevent any wrongful use, dissemination or publication of the Confidential Information not permitted hereunder by a reasonable degree of care, but no less than the degree of care used to protect its own confidential information of a like nature.

6. On receipt of a written demand from CDIC, the Supplier shall immediately return all Confidential Information, including any copies thereof, and any memoranda, notes or other documents relating to the Confidential Information (the "**Confidential Material**"), or shall provide a written certificate to CDIC certifying the destruction of all Confidential Information and Confidential Material and other materials embodying CDIC Intellectual Property if instructed by CDIC to destroy such Information.

7. The Supplier acknowledges and accepts that, in the event of any breach or anticipated breach of this Appendix, damages alone would not be an adequate remedy, and agree that CDIC shall be entitled to seek equitable relief, such as an injunction, in addition to or in lieu of damages and without being required to prove that it has suffered or is likely to suffer damages.

8. All Confidential Information is provided "AS IS" and without any warranty, express, implied or otherwise, regarding its accuracy.

9. Unless expressly authorized in this Agreement or by CDIC in writing, Supplier shall, in accordance with reasonable industry standards, enforce policies, procedures and access control mechanisms to prevent the merger, linking or commingling of any Confidential Information or Personal Information with its own data or the data of any other person;

Privacy:

10. If CDIC intends to provide the Supplier with (or allow the Supplier to access or collect on CDIC's behalf) any Personal Information as part of the Services, CDIC shall advise the Supplier of this fact, and the Supplier shall be required to comply with the following privacy obligations.

11. The Supplier shall comply at all times with all applicable Canadian laws and regulations relating to the collection, creation, use, storage and disclosure of Personal Information, and for greater certainty shall conduct itself so as to ensure that the Services comply with the Canadian *Privacy Act*.

12. The Supplier shall provide a copy of, or, where appropriate, a reference to, a privacy notice in a form acceptable to CDIC when collecting Personal Information on behalf of CDIC.

13. The Supplier shall not use or disclose any Personal Information except to the extent required to perform obligations under the Agreement or as otherwise permitted under applicable law. If, in performing its obligations under the Agreement, the Supplier is required to disclose Personal Information to a third party, the Supplier shall, prior to disclosing such Personal Information, advise CDIC in writing of the proposed use of the Personal Information by the third party. If CDIC consents to the disclosure, the Supplier shall require the third party to enter into an agreement imposing obligations upon the third party with respect to the collection, use and disclosure of the Personal Information that are substantially similar to the obligations set out herein, failing which, the Personal Information shall not be disclosed except in accordance with applicable law.

14. The Supplier shall promptly notify CDIC in writing and assist CDIC in resolving any claim, inquiry, active or pending investigation, complaint that is made to the Supplier or filed with competent authorities, or any remedial action that either has been ordered to take by competent authorities regarding the collection, storage, use or disclosure of Personal Information by the Supplier.

15. The Supplier shall retain the Personal Information only for so long as is reasonably necessary to complete the purposes for which the Personal Information was provided and as otherwise permitted by applicable law, unless otherwise specified by CDIC in writing (collectively, the "**Retention Period**") – and upon the expiry of the Retention Period, shall return to CDIC, or as directed by CDIC, delete or destroy the Personal Information. The Retention Period shall (unless otherwise specified by CDIC in writing) automatically expire on the date on which the Agreement expires or is terminated for any reason whatsoever. Upon request, the Supplier shall provide CDIC with a written certificate certifying the destruction of the Personal Information or the return to CDIC of all Personal Information (as applicable).

Conflict of interest:

16. CDIC requires any persons entering into any agreement with CDIC, supplying services to, or performing any work for or in regards to CDIC, to conduct their affairs in such a way as to avoid any conflict of interest. The Supplier hereby represents and declares that, after due inquiry, it is not aware of any circumstances which do or might cause the Supplier to have a conflict of interest in carrying out the Services. The Supplier agrees not to enter into any contract or other commitment with any person during the term of the Agreement that would cause a conflict of interest on the Supplier's part in connection with the performance of the Services.

Security:

Protection of Information

17. The Supplier confirms that Services involving Personal Information or other "**Protected Information**", as that term is defined in CDIC's *Information Classification Standard* will be handled in accordance with CDIC's *IT Asset and Information Handling Standard* and *Cryptography Procedure* and other security procedures, as applicable. Where the Supplier cannot meet the requirements of the procedure, Services involving Personal Information or other Protected Information will be performed on CDIC's premises only, using CDIC computer systems exclusively or, where applicable, specific remote access or other technology approved by CDIC in writing ("Access Technology" as set out below). The Supplier shall require that no Protected Information is removed from CDIC premises at any time during the Term of the Agreement, except where transmitted using the Access Technology.

CDIC has adopted Access Technology as a means for the secure electronic transmission of designated information, classified up to a Protected "B" level, over the Internet. In order for CDIC to provide Access Technology accounts to any Assigned Persons, the Supplier agrees that the Supplier shall, in addition to any other term herein, use the Access Technology in accordance with the following terms and conditions:

(i) CDIC shall designate one or more Assigned Persons to be known as Token Registration Authorities ("**TRAs**") who shall be responsible for coordinating the applications by, and for verifying the identify of, each Assigned Person for whom CDIC agrees to provide an Access Technology account;

(ii) CDIC reserves the right to refuse to issue an Access Technology account to any or all Assigned Persons;

(iii) Supplier shall be required to complete application forms to obtain Access Technology tokens with the approval of CDIC, together with training to be provided by CDIC concerning the administration of the Access Technology;

(iv) The Supplier shall require all Assigned Persons with Access Technology accounts to keep their respective Access Technology tokens and passwords confidential, and to take all reasonable measures to prevent the loss, unauthorized disclosure, modification or improper use of any Access

Technology token or associated password;

The Supplier shall prohibit each Assigned Person from sharing their Access Technology token or associated password with any other person;

(v) The Supplier shall require that all CDIC data accessed and modified by the Supplier and its Assigned Persons while using the Access Technology is re-saved only to the CDIC network. The Supplier and its Assigned Persons shall not transfer, save or send any copies of CDIC data to a non- CDIC computer system, nor create hard copies of the data, without the express written consent of CDIC;

(vi) The Supplier shall promptly advise CDIC if any Assigned Person's Access Technology token or associated password is, was or may be compromised or not secure, and shall likewise require Assigned Persons to promptly report any such incidents to the Supplier;

(vii) The Supplier shall promptly advise CDIC if (a) any Assigned Person ceases to be involved in providing the Services or (b) any of the information contained in an Assigned Person's Access Technology application changes or becomes otherwise inaccurate or incomplete;

(viii) The Supplier acknowledges and agrees that the Access Technology is for the sole use of the Supplier in connection with the delivery of the Services to CDIC. The Supplier shall not permit anyone other than an approved Assigned Person and CDIC to access the Access Technology and related software, or to authenticate Access Technology passwords in accordance with this Agreement;

(ix) The Supplier shall require that any operating software and computer virus software that is installed on all computer systems to be used by the Assigned Persons in connection with the Access Technology is acceptable to CDIC, and will update or install such software as CDIC may request to maintain the security of the Protected Information. The Supplier acknowledges that if the software required by CDIC is not installed properly on any computer systems used by Assigned Persons in connection with the Services, then access to the Access Technology and the CDIC network, and any use of the Access Technology , may be denied and will be at the Supplier's risk;

(x) CDIC reserves the right to revoke or modify any Access Technology account provided to any Assigned Person at any time, without notice and in its sole discretion, including without limitation if a Access Technology token or password was, is or is suspected of being compromised, or if an Assigned Person is no longer involved in providing the Services. All Access Technology accounts shall be revoked by CDIC and all Access Technology tokens promptly returned by the Supplier when the Agreement between CDIC and the Supplier expires or is terminated, whichever occurs earlier;

(xi) The Supplier acknowledges that the Access Technology software is subject to intellectual property licenses and restrictions and agrees to adhere to the terms and conditions outlined in this Agreement concerning the use of such software.

In particular, and without limiting the generality of other provisions in this Agreement, the Supplier shall not tamper with, alter, destroy, modify, reverse engineer, decompile, or abuse the Access Technology software or tokens in any way, nor distribute or use the software or tokens for any purpose other than for dealings with CDIC;

(xii) The Supplier acknowledges and agrees that it shall be jointly and severally liable with each Assigned Person for any breach of the above terms concerning the use of the Access Technology software by any such Assigned Person; and

(xiii) CDIC cannot warrant or represent that the Access Technology will be always available or functional, including without limitation because of events such as system maintenance and repair, or events outside the reasonable control of CDIC, or that occurred without the fault or neglect of CDIC.

Security Clearance

18. If the performance of the Services involves Personal Information or other Protected Information, the Supplier shall require that all the Assigned Persons or any Subcontractors' personnel who will perform the Services either:

(a) as of the Commencement Date, have a minimum security clearance of "Reliability", as that term is defined in CDIC's *Personnel Security Standard* or such other security clearance level as requested by CDIC; or

(b) within one (1) week of the Commencement Date, the Supplier will apply to obtain the necessary security clearance.

The Supplier agrees that once the required level of security clearance is obtained by an Assigned Person or any Subcontractor's personnel, it shall cause each Assigned Person or Subcontractor's personnel to maintain his or her respective security clearance for the duration of his or her work during the term of the Agreement.

Appendix D
SERVICE REQUEST FORM

(SAMPLE ONLY)

All correspondence and invoices **MUST** show the Service Request Number and Professional Services Agreement number.

<table>
<tr><th colspan="2">SECTION 1: TO BE COMPLETED BY CDIC</th></tr>
<tr><td>Service Request Number:</td><td>Professional Services Agreement Number:</td></tr>
<tr><td>Service Request Type: <Select One of the following>
☐ Direct
☐ Mini-Quotation (issued to multiple Suppliers)</td><td>Service Request Title:</td></tr>
<tr><td rowspan="2">To: <Supplier Name and Address></td><td>Date of Service Request Issuance:</td></tr>
<tr><td>Response Required by: <Identify Date and Time></td></tr>
<tr><td rowspan="2">Type of Service Requested: <Select One of the following>
☐ Service Stream #1 - Staff Augmentation Services
☐ Service Stream #2 – Project Delivery Services</td><td>Required Commencement Date:</td></tr>
<tr><td>Required Completion Date:</td></tr>
<tr><td colspan="2">Statement of Work Details: <Insert Task Details – required Work, formats, milestones or due dates, or request the Supplier to provide a work plan, as applicable></td></tr>
<tr><td colspan="2">
<table>
<tr><th>Resource/Work Required for Delivery</th><td>Identify Required Delivery Dates (if applicable):</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
</td></tr>
<tr><td colspan="2">Required Resource Roles and Levels: <Select One of the following options. Where CDIC requires specific Roles/Levels, complete the table as applicable to the requirement>

☐ Supplier to propose Resource Team</td></tr>
</table>

OR

☐ CDIC requires the Services of the following:

Role	Level	Quantity Required <*indicate number of Resources required*>	Specific Assigned Person Required <*Indicate name(s) if applicable*>

Additional Resource Requirements: <*Where CDIC requires additional experience, education/certification or qualification requirements, describe what is required per Resource Role and Level, as applicable*>

Authorized Location(s) of Work: <*Select all that apply*>

☐ On-Site (50 O'Connor Street, Ottawa)

☐ On-Site (79 Wellington Street West, Suite 1200, Toronto)

☐ Off-Site (Supplier's Premises)

Provide any additional Requirements for the Statement of Work: <*as applicable, include detailed schedule, milestones, and payment frequency (e.g. monthly, quarterly, by milestone, upon completion, etc.)*>

Service Request Response Details:
With its response to this Service Request Form, the Supplier is requested to provide the following documentation under a separate cover: **<*Select all that apply*>**

☐ Proposed Work Plan and Schedule
☐ CVs of proposed Assigned Persons (Resources) demonstrating the Minimum Qualifications for the Role and level in which they are proposed, and any additional Resource Requirements set out in this Service Request
☐ Estimated hours to complete the Services
☐ Other <***Specify***> _____

Mini-Quotation Process: <*For use when the Service Request is issued to multiple Suppliers for a Response. Select applicable options and complete as applicable to the Service Request. Delete this section if not applicable*>

Responses to this Service Request will be evaluated based on the following:
☐ Experience of proposed Assigned Persons (Resources), weighted at <__%>
☐ Proposed Total Fee, weighted at <__%>

Refined Proposal Process Details: <*Select applicable options and complete as applicable to the Service Request. Delete this section if not applicable*>

Following CDIC's review and assessment of the Supplier's initial response, the Supplier will be asked to provide a refined response (e.g. refinement of proposed Resources, work plan and effort required) for CDIC's final evaluation and selection.

Select applicable Options:

☐ For Direct Service Requests: CDIC requests the Supplier to submit a Refined Response to Service Request No. <_____###> in accordance with the updated Service Request Requirements as detailed herein <***Select where the Service Request is re-issued with refined scope, requirements, etc***.>

☐ For Mini-Quotation Process: Following the issuance of additional Refined Response Submission Requirements to Suppliers by CDIC, Suppliers will be eligible to submit a refined response for evaluation and determination by CDIC.

SECTION 2: TO BE COMPLETED BY SUPPLIER (CDIC TO SELECT APPLICABLE SUPPLIER ON BASIS OF PAYMENT).

Response Payment Format <CDIC to *select applicable Basis of Payment(s) for the Service Request and delete those that do not apply. Additional rows may be added as required*>

A. Payment on an Hourly Basis (Payment based on Actual Hours of Service Delivered multiplied by Hourly Rate)

Assigned Person Name	**Role and Level**	***Proposed Hourly* Rate**	**No. of hours**	**Extended price for Statement of Work** *(hourly rate x no. of hours)*
		$		**$**
		$		**$**
		$		**$**
			Estimated Total Fee	**$**

B. Payment on an Estimated Price Basis (Payment based on Actual Hours of Service Delivery to an overall maximum Total Fee not to exceed the total amount identified below)

Work Product	**Estimated Price per Work Product**	**Estimated number of hours per Work Product**	**Estimated extended price for Statement of Work**
	$		**$**
	$		**$**
	$		**$**
	$		**$**
		Estimated Total Fee	**$**

C. Payment on a Firm/Fixed Price Basis (Payment based on Firm/Fixed Price per Work Product to an overall maximum Total Fee not to exceed the total amount identified below)

Work Product	**Firm/Fixed Price per Work Product** *(hourly rate x no. of hours)*
	$
	$
	$
	$
	$
	$
	$
Firm/Fixed Total Fee	**$**

SECTION 3: TASK AUTHORIZATION

Both parties must provide approval in writing below, resulting in a Task Authorization, to authorize Services to commence.	
Start Date:	**End Date:**
We acknowledge receipt of this Service Request # ____ and agree to deliver the Services in accordance with the Terms and Conditions of the Professional Services Agreement and this Service Request. *I have authority to bind the Supplier:* **Supplier Signature:** _____ **Supplier Authorized Representative Name:** **Name: _____** **Date: _____**	Supplier is authorized to deliver the Services detailed in this Service Request, in accordance with its Service Request Response dated (_____). Signed, sealed and delivered on behalf of CDIC **CDIC Signature:** _____ **CDIC Authorized Representative Name:** **Name: _____** **Date: _____**