RETURN BIDS TO :

RETOURNER LES SOUMISSIONS À:

Bid Receiving Shared Services Canada | Services partagés Canada
180 Kent Street
Ottawa, Ontario
K1G 4A8
13th Floor

REQUEST FOR PROPOSAL

DEMANDE DE PROPOSITION

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

Proposition aux: Services partagés Canada
Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées **Instructions : See Herein**
ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction **Instructions: Voir aux présentes**
énumérés ici sur toute feuille ci-annexées, au(x) prix indiqué(s**)**

Comments - Commentaires

This document contains a Security Requirement

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

Issuing Office – Bureau de distribution

Shared Services Canada – SA Authority
Procurement Operations
180 Kent Street
Ottawa, Ontario
K1G 4A8

Title – Sujet
Professional Services - Service Desk, Enterprise Command Centre and Data Centre Operations Services

Solicitation No. – N° de l'invitation	**Date**
2B0KB-17-3174	11-September-2017

Client Reference No. – N° référence du client
3174

Buy & Sell Reference No. – N° de reference de SEAG
2B0KB-17-3174

File No. – N° de dossier	
2B0KB-17-31274	

Solicitation Closes – L'invitation prend fin **at – à 2 :00 PM** **on – le 13-October-2017**	**Time Zone** **Fuseau horaire** Daylight Saving Time DST

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

Address Inquiries to : - Adresser toutes questions à:	**Buyer Id – Id de l'acheteur**
Julie Watson-Bampton	**C09**

Telephone No. – N° de téléphone :	**FAX No. – N° de FAX**
613-790-5915	**613-948-0990**

Destination – of Goods, Services, and Construction:
Destination – des biens, services et construction :
See Herein

Delivery required - Livraison exigée	**Delivered Offered – Livraison proposée**
See Herein	

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

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

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

Signature **Date**_____

REQUEST FOR PROPOSAL

SERVICE DESK, ENTERPRISE COMMAND CENTRE AND DATA CENTRE OPERATIONS SERVICES FOR

SHARED SERVICES CANADA

TABLE OF CONTENTS

List of Annexes to the Resulting Contract:

List of Attachments to Part 3 (Bid Preparation Instructions):

List of Attachments to Part 4 (Evaluation Procedures and Basis of Selection):

Forms:

Form 1 - Bid Submission Form
Form 2 - Client Reference Verification Form for Mandatory Technical Criteria
Form 3 - Client Reference Verification Form for Point-Rated Technical Criteria
Form 4 - Substantiation of Technical Compliance Form
Form 5 - Code of Conduct Certification Form

PART 1 GENERAL INFORMATION

1.1 Introduction

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

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

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

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

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

Part 5 Certifications: includes the certifications to be provided;

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

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

The annexes include the Statement of Work and its appendices, Basis of Payment, Security Requirements Checklist, Federal Contractors Program for Employment Equity – Certification, and Insurance Requirements.

1.2 Summary

This bid solicitation is being issued by SSC. The resulting contract will be used by Shared Service Canada as a task base contract to provide Service Desk, Monitoring and Operational professional Services.

The professional services resources required will be responsible to provide support for the following areas:

The Enterprise Service Desk ("ESD") uses a desk to desk model. The ESD is the first point of contact for all customer Service Desks. The service includes the fulfilment of service requests as well as incident management which includes ticket creation, escalation, and resolution wherever possible.

The Enterprise Service Desk currently provides services for the 43 customers of Shared Services Canada, as well as other client departments/agencies of the Government of Canada, on a 24 hours a day, 7 days a week basis. It serves as the national escalation point of contact for all tickets from the various partner and department service desks. The ESD is also the interface to third-party vendors and operates as the after-hour partner and department service desk responsible for incident creation, escalation, and resolution.

End User Service Desk (EUSD)

SSC's End User Services operates one Service Desk supporting the desktop environment for multiple customer departments. The service desk is currently staffed as indicated in Section 2.3 with the potential of expanding to 24 hours a day, 7 days per week. The operation of the Service Desk provides national support for all clients, The service includes the fulfilment of service requests as well as incident management which includes ticket creation, escalation, and resolution wherever possible In the event

Service Desk Agents are unable to resolve the client issue or fulfil the client's request, it will be escalated to the appropriate support group(s) for resolution. The End User Service Desk agents are dedicated to their specific client.

Enterprise Command Centre (ECC)

The ECC scope encompasses a wide variety of platforms, and applications in order to manage the complex environment of SSC.

ECC provides support for: Event Management Mainframe, Event Management Midrange, and network monitoring and support. The additional duties include tape and facilities management. For this contract, ECC activities takes place in three major data centres, with onsite teams 24 hours a day, seven days a week, including holidays. The Aviation Parkway Data Centre ("APDC"), the King Edward Data Centre ("KEDC"), and the MacDonald Cartier Data Centre ("MCDC"), which is located in the National Capital Region ("NCR").

This Contract is to provide shared services to its clients, that include SSC itself, those government institutions for whom SSC's services are mandatory at any point during the Contract Period, and those other organizations for whom SSC's services are optional at any point during the Contract Period and that choose to use those services from time to time. It is intended to result in the award of a contract for 3 years, plus 3 – 1 year (s) option periods. This bid solicitation does not preclude Canada from using another method of supply for entities of the Government of Canada with the same or similar needs.

There is a security requirement associated with this requirement. For additional information, see Part 6 – Security and Financial Requirements, and Part 7 - Resulting Contract Clauses. Bidders should consult the "Security Requirements on PWGSC Bid Solicitations - Instructions for Bidders" document on the Departmental Standard Procurement Documents (http://www.pwgsc.gc.ca/acquisitions/text/plain/plain-e.html#top) Website.

On July 12, 2012, the Government of Canada announced on the Government Electronic Tendering Service that it had invoked the National Security Exception under the trade agreements in respect of procurements related to email, networks and data centres for Shared Services Canada. As a result, this requirement is subject to the National Security Exception.

Bidders must provide a list of names, or other related information as needed, pursuant to section 01 of the Standard Instructions 2003

For services requirements, Bidders in receipt of a pension or a lump sum payment must provide the required information as detailed in article 3 of Part 2 of the bid solicitation.

There is a Federal Contractors Program (FCP) for employment equity requirement associated with this procurement; see Part 5 – Certifications, Part 7 – Resulting Contract Clauses and the annex named Federal Contractors Program for Employment Equity – Certification

1.3 Conflict of Interest – Unfair Advantage

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

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

(b) if the Bidder, any of its subcontractors, any of their respective employees or former employees had access to information related to the bid solicitation that was not available to other bidders and that would, in Canada's opinion, give or appear to give the Bidder an unfair advantage.

The experience acquired by a bidder who is providing or has provided the goods and services described in the bid solicitation (or similar goods or services) will not, in itself, be considered by

Canada as conferring an unfair advantage or creating a conflict of interest. This bidder remains however subject to the criteria established above.

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

1.4 Debriefings

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

PART 2 BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

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

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

(c) The 2003 (2016-04-04) Standard Instructions - Goods or Services - Competitive Requirements are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003 and this document, this document prevails. All references to PWGSC contained within the Standard Instructions will be interpreted as a reference to SSC. All references to joint venture contained within the Standard Instructions are deleted.

(d) Section 3 of the Standard Instructions – Goods and Services – Competitive Requirements 2003 is amended as follows: delete “Pursuant to the *Department of Public Works and Government Services Act*, S.C. 1996, c.16”

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

Delete: sixty (60) days

Insert: one hundred and eighty days (180) days

(f) Section 7 is replaced by the following:

1. A bid delivered to the specified address after the closing date and time but before the contract award date may be considered, provided the bidder can prove the delay is due solely to a delay in delivery that can be attributed to a Delivery Service Company. Delivery Company means an incorporated courier company, Canada Post Corporation, or a national equivalent of a foreign country). The only pieces of evidence relating to a delay that are acceptable are:
   a) a cancellation date stamp; or
   b) a courier bill of lading; or
   c) a date stamped label

   that clearly indicates that the bid was received by the Delivery Company before the bid closing date.
2. Postage meter imprints, whether imprinted by the Bidder or the Delivery Company are not acceptable as proof of timely mailing.

(a) Section 17 of the Standard Instructions – Goods and Services – Competitive Requirements 2003 is deleted in its entirety.

(b) For purposes of this procurement the PWGSC policies referenced within the Standard Acquisitions Clauses and Conditions Manual are adopted as SSC policies.

2.2 Submission of Bids

(a) Bids must be submitted to Shared Services Canada by the date, time and place indicated on page one (1) of the bid solicitation.

(b) Due to the nature of the RFP solicitation, responses delivered by facsimile or electronically will not be accepted.

(c) Vendors intending to submit a bid are requested to notify the Contracting Authority by email (email address can be found on page 1 of the solicitation document), prior to the bid closing date, indicating their intention to submit a bid.

2.3 Former Public Servant

(a) Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts with FPS, bidders must provide the information required below before contract award.

(b) **Definitions**

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

a. an individual;

b. an individual who has incorporated;

c. a partnership made of former public servants; or

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

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

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

(c) **Former Public Servant in Receipt of a Pension**

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

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

a. name of former public servant;

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

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

(d) **Work Force Adjustment Directive**

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

If so, the Bidder must provide the following information:

a. name of former public servant;

b. conditions of the lump sum payment incentive;

c. date of termination of employment;

d. amount of lump sum payment;

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

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

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

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

2.4 Enquiries - Bid Solicitation

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

(b) Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a "proprietary" nature must be clearly marked "proprietary" at each relevant item. Items identified as proprietary will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the questions or may request that the Bidder do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 Applicable Laws

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

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

2.6 Improvement of Requirement During Solicitation Period

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

2.7 Volumetric Data

The Total Estimated # of Resources Required (per year) data has been provided to Bidders to assist them in preparing their bids. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of number of resources per year will be consistent with this data. It is provided purely for information purposes.

PART 3 BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

(a) Canada requests that Bidders provide their bid in separately bound sections as follows:

(i) Section I: Technical Bid (3 hard copies and 3soft copies on CDs or DVDs)

(ii) Section II: Financial Bid (1 hard copy and 1 soft copy on CD or DVD)

(iii) Section III: Certifications (1 hard copy and 1 soft copy on CD or DVD)

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

In the event of a discrepancy between the wording of the electronic version and the paper version, the wording of the paper version will take precedence over the wording of the electronic version

(b) Multiple bids from the same Bidder (or a bid from a Bidder and another bid from any of its affiliates) are not permitted in response to this bid solicitation. Each Bidder must submit only a single bid. For the purpose of this bid solicitation, individual members of a joint venture cannot participate in another bid, either by submitting a bid alone or by participating in another joint venture. If any Bidder submits more than one bid (or an affiliate also submits a bid), either on its own or as part of a joint venture, Canada will choose in its discretion which bid to consider.

3.2 Section I: Technical Bid

(a) The Technical Bid consists of the following:

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

(ii) **Substantiation of Technical Compliance**: The Technical Bid must substantiate the compliance with the specific Attachment form 2, which is the requested format for providing the substantiation. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Bidder will meet the requirements and carry out the required Work. Simply stating that the Bidder complies is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be considered non-responsive and disqualified. The substantiation may refer to additional documentation submitted with the bid - this information can be referenced in the "Bidder's Response" column of Attachment form 2, where bidders are requested to indicate where in their bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.

(iii) **Customer Reference Contact Information**: The Bidder must provide customer references who must each confirm if requested by SSC that Bidder meets mandatory criteria, as specified in Section 4.2 Technical Evaluation.

The Reference Project Verification Form for Mandatory Technical Criteria (Form 2) and Reference Project Verification Form for Point Rated Technical Criteria (Form 3) should be used to request confirmation from customer references.

For each customer reference, the Bidder must, at a minimum, provide the name and email address for a contact person. Bidders are also requested to include the title of the contact person. It is the sole responsibility of the Bidder to ensure that it provides a contact who is knowledgeable about the services the Bidder has provided to its customer and who is willing to act as a customer reference.

Crown references will be accepted.

.

3.3 Section II: Financial Bid

(a) Pricing: Bidders must submit their financial bid in accordance with Attachment 3.1: Pricing Tables. The total amount of Goods and Services Tax or Harmonized Sales Tax must be shown separately, if applicable. Unless otherwise indicated, all prices must be firm, all inclusive prices.

(b) **Variation in Professional Services Resource Rates from Year to Year:** If the Bidder proposes different rates for resources for different years of the resulting contract, including option years, the difference from one year to the following year must be no more than 5%.

(c) All Costs to be Included: The financial bid must include all costs for the requirement described in the bid solicitation for the entire Contract Period, including any option periods. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation and the associated costs of these items is the sole responsibility of the Bidder.

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

3.4 Section III: Certifications

Bidders must submit the certifications required under Part 5.

PART 4 EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the evaluation criteria. There are several steps in the evaluation process, which are described below. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.

(b) An evaluation team composed of representatives of Canada will evaluate the bids. Canada may hire any independent consultant, or use any Government resources, to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

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

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

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

verify any or all information provided by the Bidder in its bid; OR

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

the Bidder must provide the information requested by Canada within 2 working days of a request by the Contracting Authority.

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

4.2 Technical Evaluation

(a) Mandatory Technical Criteria: Each bid will be reviewed to determine whether it meets the mandatory requirements of the bid solicitation. All elements of the bid solicitation that are mandatory requirements are identified specifically with the words “must” or “mandatory”. Bids that do not comply with each and every mandatory requirement will be considered non-responsive and be disqualified. The mandatory evaluation criteria are described in Attachment 4.1 Technical Criteria

(b) Point-Rated Technical Criteria: Each bid will be rated by assigning a score to the rated requirements, which are identified in the bid solicitation by the word “rated” or by reference to a score. Bidders who fail to submit complete bids with all the information requested by this bid solicitation will be rated accordingly. Bids that do not obtain the required pass mark of 70% for the point-rated technical criteria specified in this bid solicitation will be considered non-responsive and be disqualified. The rated evaluation criteria are described in Attachment 4.1 Technical Criteria

(c) **Corporate References:** For Reference checks, Canada will conduct the reference check in writing by e-mail using Reference Form 2 and 3. Canada will send all e-mail reference check requests to contacts supplied by all the Bidders on the same day. For all Rated Requirements, Canada will not award any points unless the response is received within 5 Federal Government Working days (FGWDs). On the third FGWD after sending out the emails, If Canada has not received a response, Canada will notify the Bidder by e-mail, to allow the Bidder to contact its reference directly to ensure that it responds to Canada within the 5 FGWD. Wherever information

provided by a reference differs from the information supplied by the Bidder, the information supplied by the references will be the information evaluated. Points will not be allocated if the reference customer affiliate of the Bidder). Nor will points be allocated if the customer is itself an affiliate or other entity that does not deal at arm's length with the Bidder. A bidder responsive will be declared non-responsive and be disqualified if the reference from the Bidder does not confirm that the Bidder has met the Mandatory requirement(s). Crown references will be accepted.

4.3 Financial Evaluation

The financial evaluation will be conducted by calculating the Evaluated Financial Score using the Pricing Tables completed by the bidders in Attachment 3.1 Pricing Tables.

(a) The financial evaluation will be conducted by calculating the Total Bid Price using the Pricing Tables completed by the bidders.

(i)Total Bid Price is calculated as follows:

Part 1: Per Diem Rate x the number in the for Baseline Volume (Evaluation Purposes) column x the number in the FGWD and then Grand Total of Sum (Contract Period + Option periods)

Part 2: Total Bid Price for Transition Costs is the Sum of all cost as per Attachment 3.1 – Transition Cost line item 6-27

The Sum of all costs A + B = Total Bid Price

Formulae in Pricing Tables

If the pricing tables provided to bidders include any formulae, Canada may re-input the prices provided by bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by bidder.

(b) Le prix de la soumission sera évalué en dollars canadiens, excluant la taxe sur les produits et services (TPS) et la taxe de vente harmonisée (TVH) et incluant FAB destination, les droits de douane et la taxe d'accise

(c) Substantiation of Professional Services Rates

In Canada's experience, bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates bid for professional services, Canada may, but will have no obligation to, require price support in accordance with this Article. If Canada requests price support, it will be requested from all otherwise responsive bidders who have proposed a rate that is at least 15% lower than the median rate bid by all responsive bidders for the relevant resource category or categories. If Canada requests price support, the following information is required:

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

(b) in relation to the invoice in (4.3.5.1), evidence from the bidder's customer that the services identified in the invoice include at least 50% of the tasks listed in the Statement of Work for the category of resource being assessed for an unreasonably

low rate. This evidence must consist of either a copy of the contract (which must describe the services to be provided and demonstrate that at least 50% of the tasks to be performed are the same as those to be performed under the Statement of Work in this bid solicitation) or the customer's signed certification that the services subject to the charges in the invoice included at least 50% of the same tasks to be performed under the Statement of Work in this bid solicitation);

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

(d) the name, telephone number and, if available, email address of a contact person at the customer who received each invoice submitted under (4.3.5.1), so that Canada may verify any information provided by the Bidder.

Once Canada requests substantiation of the rates bid for any resource category, it is the sole responsibility of the Bidder to submit information (as described above and as otherwise may be requested by Canada, including information that would allow Canada to verify information with the resource proposed) that will allow Canada to determine whether it can rely, with confidence, on the Bidder's ability to provide the required services at the rates bid. If Canada determines that the information provided by the Bidder does not adequately substantiate the unreasonably low rates, the bid will be declared non-responsive.

4.4 Total Bid Score:

The Total Technical merit Score possible is 70% and the Total Financial Score possible is 30%

Total Technical Score + Total Financial Score = Total Bid Score

4.5 Basis of Selection

To be declared responsive, a bid must:

a. comply with all the requirements of the bid solicitation;
b. meet all Corporate mandatory Technical evaluation criteria; and
c. obtain the required minimum of 70% for Corporate Technical Rated Criteria

Bids not meeting (a), (b) and (c) will be declared non-responsive.

The evaluation will be based on the highest responsive combined rating of technical merit and price. The ratio will be 70% for the technical merit and 30% for the price.

To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows: total number of points obtained / maximum number of points available multiplied by the ratio of 70%.

For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.

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

If more than one bidder is ranked first because of identical overall combined Total Score, the bidder with the lowest Total Bid Price will become the top-ranked bidder

An example is given below for illustration purposes. Based on the calculations provided, a contract would be awarded to Bidder 3 which offers the highest total overall score taking into consideration both the technical merit and the price of the bidder's proposal.

TABLE – Example of Selection Method (Best Value Determination)			
Highest Combined Rating Technical Merit (70%) and Price (30%)			
	Compliant Bidders (Minimum technical points required: 65)		
	Bidder 1	**Bidder 2**	**Bidder 3**
Total Technical Points	55	60	65
Total cost per Attachment 3.1 Table for Resource Categories for All Identified Contract Periods	$12,500,000.00	$15,000,000.00	$18,000,000.00
Total Transition Cost	$2,000,000.00	$1,000,000.00	1,500,000.00
Total Resource + Transition Cost	$14,500,000.00	$16,000,000.00	$19,500,000.00
Maximum Technical Score: 65		**Minimum Total Resource + Transition Cost:** $14,500,000.00	
Calculation	**Technical Points**	**Price Points**	**Total Points**
Bidder 1	(55/65) x 70 = 59.23	($14,500,000 / $14,500,000) x 30 = 30	89.23
Bidder 2	(60/65) x 70 = 64.62	($14,500,000 / $16,000,000) x 30 = 27.19	91.81
Bidder 3	(65/65) x 70 = 70	($14,500,000 / $19,500,000) x 30 = 22.31	92.30

PART 5 - CERTIFICATIONS

Bidders must provide the required certifications to be awarded a contract. Canada will declare a bid non-responsive if the required certifications are not completed and submitted as requested.

Compliance with the certifications bidders provide to Canada is subject to verification by Canada during the bid evaluation period (before award of a contract) and after award of a contract. The Contracting Authority will have the right to ask for additional information to verify bidders' compliance with the certifications before award of a contract. The bid will be declared non-responsive if any certification made by the Bidder is untrue, whether made knowingly or unknowingly. Failure to comply with the certifications or to comply with the request of the Contracting Authority for additional information will also render the bid non-responsive.

Certifications Required with the Bid

The certifications listed below should be completed and submitted with the bid but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, the Contracting Authority will so inform the Bidder and provide the Bidder with a time frame within which to meet the requirement. Failure to comply with the request of the Contracting Authority and meet the requirement within that time period will render the bid non-responsive.

Federal Contractors Program - Certification

(a) The Federal Contractors Program for Employment Equity (FCP) requires that some suppliers bidding for federal government contracts, valued at $200,000 or more (including all applicable taxes), make a formal commitment to implement employment equity. This is a condition precedent to contract award. If the Bidder is subject to the FCP, evidence of its commitment must be provided before the award of the Contract.

(b) Suppliers who have been declared ineligible contractors by Human Resources and Skills Development Canada (HRSDC) are no longer eligible to receive government contracts over the threshold for solicitation of bids as set out in the *Government Contract Regulations*. Suppliers may be declared ineligible contractors either as a result of a finding of non-compliance by HRSDC, or following their voluntary withdrawal from the FCP for a reason other than the reduction of their workforce to fewer than 100 employees. Any bids from ineligible contractors will be declared non-responsive.

(c) If the Bidder does not fall within the exceptions enumerated in (d)(i) or (ii) below, or does not have a valid certificate number confirming its adherence to the FCP, the Bidder must fax (819-953-8768) a copy of the signed form LAB 1168, Certificate of Commitment to Implement Employment Equity to the Labour Branch of HRSDC.

(d) Each bidder is requested to indicate in its bid whether it is:

(i) not subject to FCP, having a workforce of fewer than 100 permanent full or part-time employees in Canada;

(ii) not subject to FCP, being a regulated employer under the *Employment Equity Act*, S.C. 1995, c. 44;

(iii) subject to the requirements of FCP, because it has a workforce of 100 or more permanent full or part-time employees in Canada, but it has not previously obtained a certificate number from HRSD (because it has not bid before on requirements of $200,000 or more), in which case a duly signed certificate of commitment is required from the Bidder; or

(iv) subject to FCP-EE, and has a valid certification number (i.e., has not been declared an ineligible contractor by HRSDC).

(e) Further information on the FCP-EE is available on the following HRSDC Website: http://www.hrsdc.gc.ca/en/gateways/topics/wzp-gxr.shtml.

5.2 Former Public Servant Certification

(a) Contracts with former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny and reflect fairness in spending public funds. In order to comply with Treasury Board policies and directives on contracts with FPS, bidders must provide the information required below.

(b) For the purposes of this clause,
(i) "**former public servant**" means a former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police and includes:
(A) an individual;
(B) an individual who has incorporated;
(C) a partnership made of former public servants; or
(D) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.
(ii) "**lump sum payment period**" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.
(iii) "**pension**" means, in the context of the fee abatement formula, a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S. 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act*, 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11, the *Members of Parliament Retiring Allowances Act*, R.S., 1985, c. M-5, and that portion of pension payable to the *Canadian Pension Plan Act*, R.S., 1985, c. C-8.

(c) If the Bidder is an FPS in receipt of a pension as defined above, the Bidder must provide the following information:
(i) name of former public servant;
(ii) date of termination of employment or retirement from the Public Service.

(d) If the Bidder is an FPS who received a lump sum payment pursuant to the terms of a work force reduction program, the Bidder must provide the following information:
(i) name of former public servant;
(ii) conditions of the lump sum payment incentive;
(iii) date of termination of employment;
(iv) amount of lump sum payment;
(v) rate of pay on which lump sum payment is based;
(vi) period of lump sum payment including start date, end date and number of weeks; and
(vii) number and amount (professional fees) of other contracts subject to the restrictions of a work force reduction program.

(e) For all contracts awarded during the lump sum payment period, the total amount of fee that may be paid to a FPS who received a lump sum payment is $5,000, including the Goods and Services Tax or Harmonized Sales Tax.

(f) By submitting a bid, the Bidder certifies that the information submitted by the Bidder in response to the above requirements is accurate and complete.

5.3 Status and Availability of Resources

(a) By submitting a bid, the Bidder certifies that, should it be awarded a contract as a result of the bid solicitation, every individual proposed in its response to Task Authorizations will be available to

perform the Work as required by Canada's representatives and at the time specified in the TA or as agreed to with Canada's representatives. If for reasons beyond its control, the Bidder is unable to provide the services of an individual named in the TA, the Bidder may propose a substitute with similar qualifications and experience. The Bidder must advise the Contracting Authority of the reason for the substitution and provide the name, qualifications and experience of the proposed replacement. For the purposes of this clause, only the following reasons will be considered as beyond the control of the Bidder: death, sickness, retirement, resignation, dismissal for cause or termination of an agreement for default.

(b) If the Bidder has proposed any individual who is not an employee of the Bidder, by submitting a bid, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

5.4 Education and Experience

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

(b) All of the resources proposed must meet the minimum experience requirements detailed in the Supply Arrangement for the Category of Personnel for which they are being proposed. The SA Holder acknowledges that the Department of Public Works and Government Services Canada reserves the right to verify this certification prior to contract award or during contract performance and that untrue statements may result in the proposal being declared non-responsive or any other action which the Minister may consider appropriate.

5.5 Certification of Language – Bilingual

By submitting a bid, the Bidder certifies that, should it be awarded a contract as a result of the bid solicitation, 80% proposed resources be bilingual. Fluent means that the proposed resources must be able to communicate orally and in writing without any assistance and with minimal errors.

5.6 Code of Conduct and Certifications

By submitting a bid, the Bidder certifies, for himself and his affiliates, to be in compliance with the Code of Conduct and Certifications clause of the Standard instructions. The related documentation hereinafter mentioned will help Canada in confirming that the certifications are true. By submitting a bid, the Bidder certifies that it is aware, and that its affiliates are aware, that Canada may request additional information, certifications, consent forms and other evidentiary elements proving identity or eligibility. Canada may also verify the information provided by the Bidder, including the information relating to the acts or convictions specified herein, through independent research, use of any government resources or by contacting third parties. Canada will declare non-responsive any bid in respect of which the information requested is missing or inaccurate, or in respect of which the information contained in the certifications is found to be untrue, in any respect, by Canada. The Bidder and any of the Bidder's affiliates, will also be required to remain free and clear of any acts or convictions specified herein during the period of any contract arising from this bid solicitation.

Bidders who are incorporated, including those bidding as a joint venture, must provide with their bid a complete list of names of all individuals who are currently directors of the Bidder (See Annex D). Bidders bidding as sole proprietorship, including those bidding as a joint venture, must provide the name of the owner with their bid. Bidders bidding as societies, firms, partnerships or associations of persons do not need to provide lists of names. If the required names have not been received by the time the evaluation of

bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply will render the bid non-responsive. Providing the required names is a mandatory requirement for contract award.

Canada may, at any time, request that a Bidder provide properly completed and Signed Consent Forms (Consent to a Criminal Record Verification Form - PWGSC -TPSGC 229) (http://www.tpsgc-pwgsc.gc.ca/app-acq/forms/229-eng.html) for any or all individuals aforementioned within the time specified. Failure to provide such Consent Forms within the time period provided will result in the bid being declared non-responsive.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirement

At the date of bid closing, the following conditions must be met:

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

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

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

6.2 For additional information on security requirements, bidders should consult the "Security Requirements for PWGSC Bid Solicitations - Instructions for Bidders" (http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-eng.html#a31) document on the Departmental Standard Procurement Documents Web site.

PART 7 - RESULTING CONTRACT CLAUSES

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

Requirement

_____ (the "**Contractor**") agrees to supply to the Client the services described in the Contract, including the Statement of Work, in accordance with, and at the prices set out in, the Contract. This includes: providing professional services, as and when requested by Canada to one or more locations to be designated by Canada, excluding any locations in areas subject to any of the Comprehensive Land Claims Agreements.

7.2 Task Authorization (TA)

(a) **Purpose of a** TA: Services to be provided under the Contract on an as-and-when-requested basis will be ordered by Canada using Appendix D to Annex A - Task Authorization Request and Acceptance Form ("TA Form").

(b) **TA Procedures**: The procedures for issuing, responding to, assessing and approving Task Authorizations are described in Appendix C to Annex A.

(c) **Authority to Issue a** TA: The Contracting Authority will be the only authority to issue tasks authorizations.

(d) **Charges for Work under a** TA: The Contractor must not charge Canada anything more than the price set out in the TA unless Canada has issued a TA amendment authorizing the increased expenditure. Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before being incorporated into the Work.

(e) **Task Authorization Quotations**: The Contractor is required to submit a responsive quotation in response to every TA Form issued to it by Canada. In addition to Canada's other rights to terminate the Contract, Canada may immediately, and without further notice, terminate the Contract for default if during the Contract Period the Contractor in at least three instances has either not responded or has not submitted responsive quotations when issued a TA Form. A responsive quotation is one that is submitted within the time stated in the TA Form and meets all requirements of the TA issued, including quoting the required number of resources that meet the minimum experience and other requirements of the Categories of Personnel identified in the TA at pricing not exceeding the rates of Annex B.

(f) **Consolidation of TAs for Administrative Purposes**: The Contract may be amended from time to time to reflect all TAs issued and approved by Canada to date, to document the Work performed under those TAs for administrative purposes.

(g) **TA Reports:** The Contractor must submit to the Contracting Authority a TA report on a quarterly basis that identifies each TA issued during that quarter and its dollar value.

(h) **Period of Services:** No Task Authorizations may be entered into after the expiry date of the Contract.

7.3 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions (http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-eng.jsp) Manual issued by Public Works and Government Services Canada.

7.4 General Conditions

2035 2016-04-04, General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

The text under Subsection 04 of Section 41 – Code of Conduct and Certifications, of General Conditions 2035 referenced above is replaced by:

> During the entire period of the Contract, the Contractor must diligently update, by written notice to the Contracting Authority, the list of names of all individuals who are directors of the Contractor whenever there is a change. As well, whenever requested by Canada, the Contractor must provide the corresponding Consent Forms.

With respect to Section 30 - Termination for Convenience, of General Conditions 2003, unless already present, Subsection 04 is deleted and replaced with the following Subsections 04, 05 and 06:

4. The total of the amounts, to which the Contractor is entitled to be paid under this section, together with any amounts paid, due or becoming due to the Contractor must not exceed the Contract Price.

5. Where the Contracting Authority terminates the entire Contract and the Articles of Agreement include a Minimum Work Guarantee, the total amount to be paid to the Contractor under the Contract will not exceed the greater of

(a) the total amount the Contractor may be paid under this section, together with any amounts paid, becoming due other than payable under the Minimum Revenue Guarantee, or due to the Contractor as of the date of termination, or

(b) the amount payable under the Minimum Work Guarantee, less any amounts paid, due or otherwise becoming due to the Contractor as of the date of termination.

6. The Contractor will have no claim for damages, compensation, loss of profit, allowance arising out of any termination notice given by Canada under this section except to the extent that this section expressly provides. The Contractor agrees to repay immediately to Canada the portion of any advance payment that is unliquidated at the date of the termination.

Supplemental General Conditions

4006 2010-08-16, apply to and form part of the Contract.

7.5 Security Requirement

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER: SRCL#2B0KB-17-3174

The Contractor must, at all times during the performance of the contract, hold a valid Facility Security Clearance at the level of SECRET, issued by the Canadian Industrial Security Directorate (CISD), Public Services and Procurement Canada (PSPC).

The Contractor personnel requiring access to sensitive work site(s) must EACH hold a valid personnel security screening at the level of SECRET. The Contractor personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid RELIABILITY STATUS. .

The contractor and/or its employees MUST NOT remove any PROTECTED or CLASSIFIED information or assets from the identified work site(s).

The contractor and/or its employees MUST NOT use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data.

Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of Shared Services Canada.

The contractor and its employees must comply with the provisions of the:

a) Security of Information Act (Latest Edition);

b) Industrial Security Manual (Latest Edition).

7.6 Term of Contract

7.6. Period of the Contract

a. **Contract Period** : The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, **which includes** :
   i. The "**Initial Contract Period**", which begins on the date the Contract is awarded and ends three years later; and
   ii. the period during which the Contract is extended, if Canada chooses to exercise any options set out in the Contract.

b. **Option to Extend the Contract** :

   The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to three (3) additional one year option periods under the same terms and conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.

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

7.7 Authorities

(a) Contracting Authority

The Contracting Authority for the Contract is:

Name: Julie Bampton
Title: Manager, Procurement Operations
Shared Services Canada
Procurement and Vendor Relations
Directorate: Procurement Operations
Address: 180 Kent Street, 8th Floor, Ottawa, Ontario K1G 4A8
Telephone: 613-790-5915
Facsimile: 613-948-0990
E-mail address: julie.bampton@canada.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform

work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

(b) Technical Authority

The Technical Authority for the Contract is: **(Will be provided at contract award)**

Name: __
Title: __
Organization: _SSC_____
Address: _
Telephone:
Facsimile: ___-___-_____
E-mail address:

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

(c) Contractor's Representative
(Will be provided at contract award)
Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: ___-___-_____
Facsimile: ___-___-_____
E-mail address: _____

7.8. Payment

(a) Basis of Payment

(i) Professional services provided under a Task Authorization with a Maximum Price: For professional services requested by Canada, in accordance with an approved Task Authorization, Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA for actual time worked and any resulting deliverables in accordance with the frim all-inclusive per diem rates set out in Annex B – Basis of Payment, GST/HST extra. The per diem rate is based on a 7.5 hour workday exclusive of meal breaks. Partial days will be prorated based on actual hours worked. When actual time worked in a day is in excess of 7.5 hours, all time worked in excess of 7.5 hours will be paid based on the prorated per diem rate, for actual hours worked when written authorization from the Technical Authority or delegate was obtained before performing the work.

(ii) Pre-Authorized Travel and Living Expenses: Canada will reimburse the Contractor for its pre-authorized travel and living expenses reasonably and properly incurred in the performance of the Work (outside of the National Capital Area), at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal, private vehicle and incidental expenses provided in Appendices B,C and D of the Treasury Board Travel Directive, and with other provisions of the directive referring to ‘travelers”, rather than those referring to “employees”. All travel must have the prior authorization of the Technical Authority All payments are subject to government audit. The Contractor will be able to charge for time spent travelling.

(iii) Competitive Award : The Contractor acknowledges that the Contract has been awarded as a result of a competitive process. No additional charges will be allowed to compensate for errors, oversights, misconceptions or underestimates made by the Contractor when bidding for the Contract.

(iv) Professional Services Rates : In Canada's experience, bidders from time to time propose rates at the time of bidding for one or more Resource Categories that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. This denies Canada of the benefit of the awarded contract. If the Contractor does not respond or refuses to provide an individual with the qualifications described in the Contract (or proposes instead to provide someone from an alternate category at a different rate), whether or not Canada terminates the Contract as a whole, Canada may impose sanctions or take other measures in accordance with the PWGSC Vendor Performance Policy (or equivalent) then in effect, which may include an assessment that results in conditions applied against the Contractor to be fulfilled before doing further business with Canada, or full debarment of the Contractor from bidding on future requirements.

(v) Purpose of Estimates : All estimated costs contained in the Contract are included solely for the administrative purposes of Canada and do not represent a commitment on the part of Canada to purchase services in these amounts. Any commitment to purchase specific amounts or values of services are described elsewhere in the Contract.

(vi) On-call Rates: On-Call Services shall be performed only upon the written authorization of the Technical Authority or a delegate. The Contractor will be paid for the actual hours of the on-call period at the firm rate of 1/10 the hourly rate, as per Annex B – Basis of Payment for the Resource Categories associated with the person that is on-call. If an on-call resource is called back to perform Work by the Technical Authority or Delegate, the Contractors will be paid for the actual hours worked at the applicable per diem rate as specified in the contract**.**

(vii) Transition Professional Services provided a Task authorization with Firm Price set out in Annex B: For professional services requested by Canada, in accordance with an approved Task Authorization, Canada will pay the Contractor the firm price based on the price set out in Annex B, GST/HST extra.

Estimated Cost : [$_____]

(viii) Applicable Taxes :

Estimated Cost : [$_____]

(ix) Service Credits: Reference Appendix B to Annex A attachment

For the provision of professional services the Contractor shall refer to Appendix B to Annex A – SSC Enterprise Service Desk, End User Service Desk, Enterprise Command Center and Data Center Operation Service Level Agreement.

For each Service Level Failure, the Service Provider must provide to Shared Services Canada a Service Level Credit calculated as:

Service Level Credit = A x B

Where:

A = the CSL Allocation Percentage for the applicable CSL; and

B = the At Risk Amount.

(x) Service Level Earn Backs:

If, during the three (3) month period immediately following the month in which a Service Level Failure occurs with respect to a particular CSL, a performance is achieved that is equal to or greater than the applicable Service Level in each of those three (3) months, then the Service Provider will receive a one month credit. The credit earned back will be equal to the amount of the Service Level Credit provided to Shared Services Canada for the Service Level Failure with respect to that CSL in the month which preceded the three month period (an “Earn back Credit”).

An Earn Back Credit will offset and cancel such Service Level Credit.

7.9 Limitation of Expenditure

1. Canada's total liability to the Contractor under the Contract must not exceed $ _____ and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.
2. No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

   a. when it is 75 percent committed, or

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

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

   whichever comes first.

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

7.10 Time Verification

Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contractor must repay any overpayment, at Canada's request.

7.11 Invoicing Instructions

1. The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. Invoices cannot be submitted until all work identified in the invoice is completed.
2. The Contractor's invoice must include a separate line item for each subparagraph in the Basis of Payment Provision.
3. By submitting invoices, the Contractor is certifying that the goods and services have been delivered and the all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.
4. The Contractor must provide the original of each invoice to the Technical Authority. On request, the contractor must provide a copy of any invoices requested by the Contracting Authority.
5. In the event that Canada is entitled to a Service Credit due to any Non-Conformity, the Service Credit will be applied to the invoices to be issued to Canada in respect of the Work in question in an amount as set out in Appendix B to Annex A, In-Service & Service implantation liquidated damages from the time of the Contractor's receipt of Canada's notification of such Non-Conformity
6. The Contractor must include adjustments for Service Credits owing to Canada in the invoice that follows the month after the month in which the Service Credits accrue.
7. Each invoice must be supported by:

    a. a copy of time sheets to support the time claimed;

    b. a copy of the release document and any other documents as specified in the Contract;

    c. a copy of the invoices, receipts, vouchers for all direct expenses, and all travel and living expenses;

    d. a copy of the monthly progress report.

8. Invoices must be distributed as follows:

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

7.12 Certifications

Compliance with the certifications provided by the Contractor in its bid is a condition of the Contract and subject to verification by Canada during the term of the Contract. If the Contractor does not comply with any certification or it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

7.13 Applicable Laws

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

7.14 Priority of Documents

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

(a) the Articles of Agreement;
(b) the general conditions 2035 2014-09-25, General Conditions - Higher Complexity - Services;
(c) Annex A, Statement of Work;
(d) Annex B, Basis of Payment;
(e) Annex C, Security Requirements Check List
(g) the Contractor's bid dated _____ (insert date of bid)

7.15 Foreign Nationals (Canadian Contractor)

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

7.16 Insurance Requirements

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

7.17 Limitation of Liability

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

2. First Party Liability:

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

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

      ii. physical injury, including death.

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

   c. Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in

respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

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

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

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

   ii. any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (ii) of the greater of .75 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the block titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or $200,000.00.

   iii. In any case, the total liability of the Contractor under paragraph (e) will not exceed the total estimated cost (as defined above) for the Contract or $200,000.00, whichever is more.

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

3. Third Party Claims:

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

b. If Canada is required, as a result of joint and several liability, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite paragraph (a), with respect to special, indirect, and consequential damages of third parties covered by this section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.

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

7.18 Professional Services – General

a. The Contractor must provide professional services on request as specified in this Contract. Where in the Contract a specific individual is identified as required to perform the Work, the Contractor must make such person available to perform the work within 10 working days of the issuance of the Contract or the TA (whichever first contains instructions from Canada for that individual to report to the Work site). Where such a specific individual is unavailable to perform the Work, Canada may elect to either (i) exercise its rights or remedies under the Contract or at law (including terminating the Contract for default), or (ii) Canada may require the Contractor to propose the replacement of the specific individual in accordance with the Article titled, "Replacement of Specific Individuals" in the General Conditions 2035. This obligation applies despite any changes that Canada may have made to any hardware, software or any other aspect of the Client's operating environment. In respect of any given Category of Personnel, any replacement resource must be rated by the Technical Authority and the score obtained must be equal or superior.

c. If there must be a change in a resource performing work under the Contract (which must in any case comply with the requirements in the section of the General Conditions entitled "Replacement of Specific Individuals"), the Contractor must make the replacement available for work within 10 working days of the departure of the existing resource (or, if Canada has requested the replacement, within 15 working days of Canada's notice of the requirement for a replacement).

d. All resources provided by the Contractor must meet the qualifications described in the Contract (including those relating to previous experience, professional designation, education, and language proficiency) and must be competent to provide the required services by any delivery dates described in the Contract. The resource must be approved by Canada prior to the replacement at the Work site.

e. The Contractor must monitor its employees to ensure satisfactory performance and that progress of the Work is maintained to Canada's satisfaction. A Contractor representative must meet with the Technical Authority on a regular basis (as specified by Canada) to discuss the performance of its resources and to resolve any issues at hand.

e. If the Contractor fails to meet any of its obligations under this Article, or fails to deliver any deliverable or complete any task described in the Contract on time, in addition to any other rights or remedies available to Canada under the Contract or the law, Canada may notify the Contractor of the deficiency, in which case the Contractor must submit a written plan to the Technical Authority within 10 working days detailing the actions that the Contractor will undertake to remedy the deficiency. The Contractor must prepare and implement the plan at its own expense.

7.19 Safeguarding Electronic Media

a. Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.
b. If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

7.20 Representations and Warranties

The Contractor made statements regarding its and its proposed resources experience and expertise in its bid that resulted in the award of the Contract and issuance of TA's. The Contractor represents and warrants that all those statements are true and acknowledges that Canada relied on those statements in awarding the Contract and adding work to it through TA's. The Contractor also represents and warrants that it has, and all its resources and subcontractors that perform the Work have, and at all times during the Contract Period they must have, the skills, qualifications, expertise and experience necessary to perform and manage the Work in accordance with the Contract, and that the Contractor (and any resources or subcontractors it uses) has previously performed similar services for other customers.

7.21 Conflict of Interest - Unfair Advantage

1. In order to protect the integrity of the procurement process, bidders are advised that Canada may reject a bid in the following circumstances:

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

    b. if the Bidder, any of its subcontractors, any of their respective employees or former employees had access to information related to the bid solicitation that was not available to other bidders and that would, in Canada's opinion, give or appear to give the Bidder an unfair advantage.

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

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

7.22 Electronic Procurement & Payment Support

Electronic Procurements and Payment (EPP) System

(a) SSC is working on an initiative that is expected to provide it with e-functionality from procurement through payment (the "**EPP system**"). SSC's suppliers will be required to interface with that functionality.

(b) Because the functionality will not be ready at the time of contract award, if Canada wishes for the Contractor to interface with the EPP system during the Contract Period, Canada will issue a Request for Quotation regarding the work required for the Contractor to interface with the EPP system. The Contractor's Quotation Response will not be subject to a Service Delivery Interval. The Quotation Response must include, at a minimum:

4.4.b.1 Per diem rates for any resources who would perform the work and the level of effort required; and

4.4.b.2 Any costs for hardware or software that will be required, including development costs to be performed by third parties.

(c) The Parties agree to work cooperatively to determine the work involved and a reasonable ceiling price for that work. If the Parties agree to proceed with that work, Canada will issue a Contract Amendment documenting the ceiling price associated with the work. The Contractor will be required to submit a Service Design for approval by Canada and the work associated with the development of any EPP system interfaces will be treated as a Service Project.

(d) Canada will pay the Contractor, in arrears, up to the ceiling price established in the contract amendment, for actual time worked and any resulting deliverables in accordance with firm, all-inclusive per diem rates set out in the relevant contract amendment, with GST/HST extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday**.** When submitting its invoices, the Contractor must show the actual time worked by each resource, and/or the amount paid to any subcontractor. With respect to any expenses, the Contractor will be required to demonstrate the out-of-pocket amount spent and will be reimbursed without the addition of any overhead.

7.23 Implementation

The 30 calendar days immediately following the date of acceptance of the TIP is the Transition-In Period, during which the TIP will be implemented by the Service Provider. SSC will not change the technical infrastructures or environments identified in the RFP during the Transition-In Period. The Transition exercise is of critical importance to ensure that the Service Provider is fully capable of performing the responsibilities of the Function at Contract Start Date and to demonstrate to SSC that the expected levels of service are being achieved.

7.24 Transition of Services at end of Contract Period

At the end of the Contract Period, the Service Provider must assist with the transition of the Domain to a new Service Provider. The Service Provider must cooperate with a new Service Provider to ensure that smooth and seamless transition of services occurs. The Service Provider must ensure that overall operational availability is not disrupted; existing service levels are maintained and Contract deliverables continue to be delivered while transition and knowledge transfer to a new Service Provider occurs.

If the services are still required upon the expiry date of the contract the firm agrees to continue services at the same rate. This will be completed through a formal contract amendment authorized by the Contracting authority.

ANNEX A
STATEMENT OF WORK

PART 1
SSC END USER SERVICE DESK

1. Introduction

The scope of the Services that are the subject of this RFP are detailed in Section 4 of this document, and include the following:

- Service Management Functions (see Section 4.1 for more details);
- End User Service Desk ("EUSD") (see Section 4.2 for more details);
- Request Fulfilment (see Section 4.3 for more details);
- Transition Services (see Section 4.4 for more details).

Shared Services Canada ("SSC") has written the statement of work to focus on specific outcomes and activities the Service Provider will execute.

2. Contract Terms

2.1. Location

All services will, initially, need to be delivered from the National Capital Region (NCR). .
In the event of a disaster at the present location of operations, the Service Desk shall be reassigned to a Disaster Recovery ("DR") site within the NCR to resume operations until the situation is rectified, as per current SSC Business Continuity procedures.
It is expected that all resources will be centrally located in the NCR SSC will provide the Service Provider with sufficient notice of any facility (or service delivery location) changes. Changes to the location will not trigger a change to pricing or other expenses. Bidders are expected to take this into consideration in their pricing responses.

2.2. Workstations and Telephones

During the Contract period, SSC will provide workstations for the Service Provider's resources to use. The Service Provider will also be provided with an office phone system that includes Service Desk Agent phones. Bidders are encouraged to review the Financial Responsibility Matrix tab in the Pricing Template Attachment 3.1 for clarity on what SSC will provide and what the Service Provider is responsible for providing in their pricing submission.
The Service Provider will be responsible for providing its resources with smart phones as required at their own expense.

2.3. Operating Hours

Operating hours for the individual service desks currently are as follows:

- Public Services and Procurement Canada Service Desk
  - Weekdays: 0600 to 2100 Eastern except statutory and most civic holidays
  - Weekends: 0900 to 1700 Eastern except statutory and most civic holidays

- Shared Services Canada Service Desk
  - Weekdays: 0600 to 2000 Eastern weekdays except statutory and most civic holidays
- Health Canada Service Desk
- Weekdays: 0700 to 2000 Eastern weekdays except statutory and most civic holidays
- Canada School of Public Service Service Desk:
  - Weekdays: 0600 to 2000 Eastern weekdays except statutory and most civic holidays
- Infrastructure Canada Service Desk:
  - Weekdays: 0700 to 1700 Eastern weekdays except statutory and most civic holidays

Hours of operation are subject to change based on business requirements and direction from SSC.

2.4. Language Requirements

All End User Service Desk agents and management staff must be bilingual in English and French.
75% of the Request Fulfilment resources must be bilingual in English and French.

2.5. Security Clearance Requirements

All End User Service Desk management must obtain Level II Secret Government of Canada security clearance and maintain Level II Secret security clearance for the duration of their employment. SSC will temporarily allow Service Provider staff to provide services as long as they have received Reliability Status and have submitted an application for Level II Secret clearance. No less than 80% of the Service Provider staff delivering the services must have their Level II Secret clearance.

3. Current State Summary

Since 2010, SSC has outsourced their End User Service Desk and Request Fulfilment functions to its existing Service Provider. The contract with this Service Provider is set to expire on June 30, 2018. (The purpose of this description is to provide Proponents with context and is not intended to be an indication of how SSC would like to have their services delivered.) To be reviewed SSC and Government of Canada data currently resides in Canada and this mandatory requirement must be maintained throughout the duration of the subsequent contract.

3.1. Service Desk

SSC's End User Services operates one Service Desk supporting the desktop environment for multiple customer departments. The service desk is currently staffed as indicated in Section 2.3 with the potential of expanding to 24 hours a day, 7 days per week. The operation of the Service Desk provides national support for all clients, The service includes the fulfilment of service requests as well as incident management which includes ticket creation, escalation, and resolution wherever possible In the event Service Desk Agents are unable to resolve the client issue or fulfil the client's request, it will be escalated to the appropriate support group(s) for resolution. The End User Service Desk agents are dedicated to their specific client.

Currently the primary contact method is toll-free number with the potential of expanding to other contact channels as technologies become available.

3.1.1. Telephony

The current Service Desk telephony solution is a hosted Centrex solution provided by a third-party and accessed via the Internet. End users call a main number (specific to their organization) that is forwarded to a Control Directory Number ("CDN"). The Automated Call Distribution ("ACD") system is then controlled by client software running on a workstation communicating with the hosted solution. The Service Provider has access to monitoring and administration tools with capabilities such as, but not limited to: Registration of agents, designation of skill sets, recording and loading of broadcast messages, production of reports and monitoring of live call. Future capabilities for call recording and skill based routing will become available in 2018.

3.1.2. Remote Takeover Tools

Currently, the remote takeover tools used by the Service Desk are SCCM Client Centre and Cisco WebEx Support Centre. These tools are available to connect to virtually every end-user's production networked workstation. It is expected that all agents are trained to use these tools to ensure high First Contact Resolution service levels are achieved. The tools used for remote takeover are subject to change at SSC's discretion.

3.1.3. Knowledge Database

Atlassian Confluence is the End User Service Desk's knowledge base. The knowledge base is kept up to date as new applications, supported departments/agencies, or products are added to the environment. The knowledge base consists of common incidents with their solutions as well as lists of resolution attempts for common incident symptoms. Diagnosis methodologies are entered in this database for several incident types. It is expected that all agents are trained to use the knowledge base to ensure high First Contact Resolution service levels are achieved. The Service Provider will also be expected to contribute to the creation of new articles, as well

recommend changes to existing articles in order to keep the EUSD knowledge base current. The EUSD knowledge base tools are subject to change at SSC's discretion.

3.1.4. Incident and Change Management Tools

The Service Desk currently uses multiple IT Service Management ("ITSM") tools to manage service requests and incidents. The ITSM tools in use are subject to change at SSC's discretion.

3.2. Request Fulfilment

Request Fulfilment involves the processing of service requests that are defined as pre-approved, low risk changes to the desktop/infrastructure environments that follow standardized and documented procedures.

Currently the primary contact methods are email and an on-line portal with the potential of expanding to other contact channels as technologies become available.

3.2.1. Request Fulfilment Tools

Multiple ITSM tools are used for recording and tracking Installs, Moves, Adds and Changes ("IMACs"). The ITSM tool(s) used for Request Fulfillment is subject to change at SSC's discretion.

4. Service Descriptions

This section details the service requirements the Proponents will be expected to include in their proposal and pricing. These services do not necessarily reflect what or how services are currently delivered by the current Service Provider.

4.1. Service Management Functions

Service Management Functions Services are activities that the Service Provider must perform across all functional areas.

Where there is an impact or interaction with SSC, the Service Provider must deliver the Services using industry standard methodologies and market best practices. SSC may request documentation that provides proof of this. The Service Provider must follow relevant SSC policies and procedures.

4.1.1. Governance

The objective of Governance is to:

- monitor and ensure consistent quality for services being delivered to SSC by the Service Provider;
- proactively identify, assess and mitigate risks (both operational and reputational) to SSC stakeholders and ensure compliance to SSC policy and procedures;
- ensure interpretation and compliance to the contract and changes to the terms of the contract and/or SLAs;
- monitor and ensure consistent strategic alignment between stakeholder strategies and service requirements to the Service Provider performance;
- develop, implement, and manage processes such as call, incident, event, problem, change, service request, and domain management;
- ensure appropriate levels of engagement between internal stakeholders and the Service Provider at the right point in time in the governance processes;
- provide central reporting and proactively identify areas of improvement;

- provide a continuous improvement framework which strengthens operational performance and fosters the development and implementation of technologies that are in line with technology standards and industry best practice;

4.1.1.1. Governance Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Governance Activities	Service Provider	SSC	SSC Comments
EUSD Management			
Lead a team of professionals in the delivery of IT services such as overseeing workforce management, quality assurance and operational performance.	X		
Provide coaching to team members.	X		
Implement approved management processes.	X		
Establish mechanisms for ongoing working interfaces (e.g. daily, weekly or monthly meetings and quarterly reviews) with team members managed under the Service Desk contract as well as contractors associated with other contracts.	X		
Manage all personnel based resources in such a manner to avoid any employer-employee relationship with respect to SSC and the contractor's personnel resources. TO be reviewed based on Kristin Comment	X		
Establish the necessary management structure and related processes to ensure that all responsibilities that are specified in this SOW are carried out such that the terms and conditions are met.	X		
Participate in and /or lead projects as required.	X		
Liaise with various work units and personnel to determine resource requirements as necessary to complete project work.	X		
Manage projects to ensure that milestones are met in accordance with project guidelines.	X		
Implement processes in consultation with various work units and personnel which will track all new work and project related activities concerning Service Desk activities.	X		
Plan, manage and execute all contracted activities.	X		
Identify, define and report on workload metrics that best measure the performance of all personnel and the overall operation.	X		

Governance Activities	Service Provider	SSC	SSC Comments
Develop and implement comprehensive Monthly Action Plans (“MAP”) that identify how performance and quality issues will be resolved.	X		
Provide expertise and guidance with regards to overseeing operations providing Service Desk support.	X		
Implement corrective actions or process improvements related to call, incident, problem, escalation and change management.	X		
Determine technical workload specifications (i.e. staffing levels) in relation to the Service Desk environment.	X		
Review service management Performance reports such as quality assurance, daily and weekly call statistics, and issue/problem resolutions.	X		
Analyze Service management performance reports to determine corrective actions and process improvements in areas such as call resolution and customer service.	X		
Liaise with various work units and Personnel to address issues directly affecting day-to-day operations.	X		
Provide a mechanism to track agent utilization for those personnel’s who do not use a system that tracks agent state and/or time allocation.	X		
Work with various work units and personnel to define appropriate paths for the flow of contract information and status.	X		
Provide a mechanism for all Service Desk personnel to call another resource for help and guidance prior to escalating to on-call resources	X		
Provide a weekend mechanism for the on-call resources to escalate issues.	X		
Notify SSC when operational documentation and procedures require updating to ensure that information is accurate, current, and complete at all times.	X		
Review all service request management interfaces and service centre categories and statuses used by the Service Desk, and recommend changes to ensure that the categories and status reflects at all	X		

Governance Activities	Service Provider	SSC	SSC Comments
times the nature and the flow of work processed.			
Train Service Desk staff according to SSC's approved training plan and curriculum. Demonstrate that effective and successful training occurred.	X		At Service Provider's expense
Provide suggestions to improve the EUSD's knowledge base accuracy and effectiveness.	X		
Perform modifications to maintain or improve knowledge base efficiency and effectiveness.		X	
Recommend functional and informational changes to the ITSM tool in order to improve overall use of the ITSM tool and performance of the Service Desk and the information passed on to support groups.	X		
Develop and implement performance monitoring processes to ensure quality service is provided and productivity targets are met or exceeded.	X		
Solicit feedback based on comments left in end user satisfaction surveys for potential service improvements.	X		
Work with the performance measurement group and incident management group in the processing and management of Customer satisfaction surveys or feedback.		X	
Review client satisfaction surveys and customer feedback to take corrective action (i.e. update documentation, address performance concern, callback customer, etc.) in response to unsatisfactory feedback.	X		
Make resources available, at any time of the day and the week, to work with the technical authority to restore regular service in case of major system and environmental problems, such as: natural disaster, virus, etc.	X		
Attend all daily and weekly service management meetings, such as the "what happened yesterday" (WHY) meetings, and provide all required status and reports in order to meet process and service management requirements.	X		
Oversee Service Desk personnel training, mentoring and coaching to ensure compliance with performance standards for: i. call etiquette ii. system access	X		

Governance Activities	Service Provider	SSC	SSC Comments
iii. creating and closing (tickets) iv. linking call records to tickets v. referencing change requests vi. escalation procedures vii. password reset viii. contingency plans ix. standard Service Desk procedures i. ESD knowledge base management and known error database			
Evaluate personnel and position them where they will be most effective to meet service level targets per the SOW.	X		
Test and execute contingency plans for critical Service Desk functions and systems.	X		
Act as a central point of contact to provide technical information such as the nature of the incident, status, technical specifications, needed for additional information between the user-client community and the IT support groups, for all requests, incidents and related activities.	X		
Implement, flag deficiencies, and suggest improvements to Service Desk procedures.	X		
Ensure that Service Desk procedures are kept current in accordance with operational directives.		X	
Manage Service Desk personnel to ensure that service levels are met as per the SLA.	X		
Monitor missed service levels to ensure performance improves.	X		

4.1.2. Reporting

The Service Provider performing any of the Service Desk functions and sub-functions must develop, deliver and maintain a system and processes for specific Workload Metrics ("WM") to: collect, store, query and report information that identifies and measures the volume, quality and service level of work performed and the resources required to perform work associated with that Service Desk function and/or sub-function. This Workload Metrics System ("WMS"), including associated reports, will provide SSC with the necessary information to fully monitor operations.

Within the first 3 months following the Contract Start Date, the Service Provider must provide to SSC its proposed WMS, including sample reports that will use specific Workload Metrics. SSC retains the right to request further development, changes and further reports from the Service Provider to be included in the WMS. SSC's approval of the WMS will be provided through written communication. The WMS and reports must be prepared and submitted to SSC every calendar month, as described below, or within 5 business days upon written notice by SSC.

At any time, SSC is entitled to access and audit any Workload Metric and performance measurement reports and systems for completeness, accuracy and content. A complete list of reports are defined in Appendix A to Annex A.

4.1.2.1. Reporting Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Reporting Activities	Service Provider	SSC	SSC Comments
Design, develop, maintain and deliver Service Desk reports on SLA and KPI's requested by SSC.	X		
Provide reporting analysts to address periodic ad hoc reporting requests regarding end user contacts and SSC information, to be approved by authorized SSC personnel.	X		
Provide access to raw data captured within the service management tool for consumption and manipulation by customer analysts and management.	X		
Track and report workload metrics on calls, incidents, problems and changes on a daily, weekly, monthly and quarterly basis.	X		
Report weekly on all activities at the Service Desk including but not limited to call metrics and service management metrics such as call, incident and change management tickets.	X		
Review daily all tickets for quality and compliance to documentation standards and administrative processing protocols.	X		
Explain and demonstrate monthly the human resource usage based on workload and metrics. Report monthly on the resource requirement for each process based on workload. Demonstrate and report that quality thresholds each indicator for each process are met.	X		
Report monthly on overall expertise, knowledge and performance levels for each specific areas of expertise such as Service Desk agents as well as account administrators.	X		
Report monthly on general performance relative to SLAs' obligations and objectives, i.e. met or not met, or the proportion of time taken by the EUSD.	X		
Report quarterly on the integrity and day-to-day procedures reviewed, indicating where the quality of work has degraded, maintained, or improved. Perform regular reviews of the day-to-day	X		

Reporting Activities	Service Provider	SSC	SSC Comments
procedures that may lead to errors, account duplication, account not in appropriate context, or inactive.			
Report weekly on all incidents resolved and not resolved at the Service Desk. Perform quality assurance (exercise quarterly and report on findings, deficiencies, degradation, problems with existing processes, procedures, or EUSD staff) and recommend corrective measures and/or any improvements.	X		
Produce monthly metrics and volumetric that demonstrates optimal performance or any required improvement in performance relating to incident resolution and request processing.	X		
Report weekly on all service requests.	X		
Report quarterly on recommendations on ways to improve handling of service requests.	X		

4.2. End User Service Desk ("EUSD")

The objectives of the End User Service Desk to:

- Operate and maintain a Service Desk operation to ensure prompt and quality desktop environment support to multiple customer departments;
- Act as a single point of contact for all user requests, and l resolve issues on first call, or route to the appropriate resolving Service Line (support group) or vendor ;
- Perform active case management be accountable for end to end delivery of requests and for ensure resolution is driven by all downstream Service Line (support groups)
- Function as the Incident Management lead to coordinate the resolution of all incidents;
- Meet SSC's service level objectives:
    - Average Speed to Answer is 70% <120 seconds and 90% <300 seconds
    - Abandon Rate is <7.5%

The Service Provider must provide Service Desk services consistent with an industry leading operation. The Service Provider must create or update a ticket for every reported incident and be responsible for updating and managing the ticket throughout its entire lifecycle. SSC will need visibility at all times to the status of tickets so they can be informed and capable of responding to questions from SSC staff.

Incidents will be reported directly to the Service Desk by phone, email or through online interfaces (i.e.portal). It will be the Service Provider's responsibility to resolve incidents on first contact and if the incident or request will be escalated, gather sufficient information to share with Service lines (support groups) or vendors. The Service Provider must perform due diligence to discover, understand and integrate with the current escalation processes between the various support teams in SSC.

SSC will provide the facilities, office equipment, voice equipment and network connectivity for the delivery of End User Service Desk services as defined in the Attachment 3.1 - Pricing Submission Sheet.

To reduce the number of Service Desk contacts, SSC provides end users the ability to resolve problems on their own. The Service Provider must proactively document solutions to common problems and, in the future .SSC will post to the SSC self-service portal where users may search for common solution.

Upon receipt of a report/incident from a supported end user or authorized SSC representative, the Service Desk must log the incident in the ITSM tool and perform an initial investigation to resolve the incident or dispatch to the appropriate support team. This will require the Service Provider to initiate hierarchical escalation within SSC and the Service Provider's organization to provide the appropriate management communication when a critical incident occurs. The resolver may be an SSC Service line (support group), a Service Provider support group or a vendor. SSC is responsible for procuring and maintaining all necessary contracts with third party vendors for which they have a direct relationship, for providing the Service Provider with all necessary vendor contact and contract information, and identifying the appropriate queue within the Ticketing System for incidents that are to be resolved by any specific SSC service line or vendor.

If the Service Provider is unable to resolve an incident upon its initial investigation, the Service Provider must route the ticket to the appropriate support team. The Service Provider must contact the appropriate support team, in the case of incidents related to the system or any services provided by Service Provider, or the appropriate SSC or third party resolver in the case of all other incidents.

SSC reserves the right to change the classification/priority/severity in cases where SSC determines the business or end-user impact is higher than initially determined by the Service Provider.

The Service Provider must perform incident analysis and diagnostics to determine the cause of the reported incident. The Service Provider must also perform ticket monitoring, re-assignment, and service level issues, as well as technical and performance analysis. The Service Provider must track and report on how much time was spent working on each ticket across each stage of the technical support lifecycle (e.g., Diagnosis, Resolution, etc.).

All Service Desk Agents must monitor, but not limited to, call, incident, and change management tickets for status updates, performing the required escalation and notification according to pre-defined procedures. The EUSD must monitor the required service management tools and other monitoring devices necessary to complete this function.

The Service Provider must provide remote support for end user devices which includes, but not limited to: desktops, laptops, tablets as well as email functionality support for smartphones. Support provided shall be consistent with industry leading processes and frameworks. The Service Provider must coordinate and work with the appropriate support groups to ensure requests are fulfilled and tickets are resolved. The Service Provider must dispatch and assign tickets to the appropriate support group and verify all activities have been completed.

4.2.1. Incident Management

For further clarification, the Service Provider is responsible for incident management for all clients of the End User Service Desk. The Service Provider must designate an on-duty incident coordinator with the responsibility for coordinating responses to significant incidents that involve outages and/or performance degradation with the Service Provider, SSC, and other technical support groups as needed. This resource must act as the primary contact between SSC and the Service Provider for resolution of these incidents.

SSC will require the Service Provider to document, report, and coordinate the resolution of all incidents. This requires the Service Provider to isolate the incident, document it and determine the full impact of the incident, including the estimated number of users impacted. The Service Provider must coordinate the incident communication of ongoing status of incidents with the

Service Desk. All communications and updates pertaining to the incident must be captured and documented within the ticket for reporting purposes. The Service Provider may be required to engage with other Third Parties for the purposes of investigation and resolution. Regardless of what caused the incident no additional fees will be charged to SSC over and above the base resource unit fees defined in the Attachment 3.1- Pricing Submission Sheet. SSC may request a written report that details the root cause, an analysis, and a procedure and/or plan for correcting incidents. In the event that the incident resolution exceeds the MTRS (Mean Time to Restore Service) service level, the Service Provider must provide options to mitigate the impact or identify temporary workarounds End User Service Desk Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

End User Service Desk Activities	Service Provider	SSC	SSC Comments
General Support			
Provide a single point of contact accessible via telephone, email address, fax, and web-enabled interfaces.	X		
Provide the Service Provider all information necessary to develop training documentation, policy guides, reference manuals, procedures and support scripts necessary for Service Desk staff and technicians to function appropriately.		X	
Provide Service Desk personnel access to a EUSD knowledge base to search for information when responding to SSC service requests and incidents.		X	
Develop and maintain training documentation based on existing operational documentation including support scripts.	X		
Maintain Service Desk operations documentation including support scripts.		X	
Identify any incidents and service requests and communicate with SSC support teams.	X		
Communicate to SSC support teams, the status of any incidents and service requests, until the incidents and service requests are resolved and closed.	X		.
Provide early warning and recommendations to SSC of incidents or problems based on information and knowledge of SSC's operating environment (e.g. common trends, new incidents, call volume spikes, etc.).	X		
Approve action/response to recommendations for incident/problem avoidance recommendations.		X	
Develop a Customer satisfaction scoring mechanism to measure SSC satisfaction with Service Desk services being provided.		X	Mechanism should have the ability to tie SSC responses to

End User Service Desk Activities	Service Provider	SSC	SSC Comments
			specific Service Desk personnel.
Approve satisfaction scoring mechanism developed.		X	
Implement the Customer satisfaction scoring mechanism as approved by SSC.	X		SSC to provide information necessary to support the implementation of the tool (i.e. communications plan).
Schedule operational reviews with SSC (monthly), and highlight opportunities or areas where process improvements could be made to improve service levels, operational performance, or providing other benefits related to Service Desk operations.	X		
Attend operational reviews with Service Provider and SSC (monthly).	X		
Provide a single point of contact who is responsible for interfacing with SSC on matters related to the Service Provider's delivery of Services.	X		SSC will approve this individual.
Identify user training needs based on patterns and frequency of contacts to the Service Desk.	X		
Manage the staff required to provide the Service Desk services.	X		
Maintain Service Desk staffing levels for planned and unplanned contact volume overflows (e.g. emergencies, enterprise application deployments etc.).	X		
Provide projected call volumes and related staffing level requirements.		X	
Take into account the peak volume periods caused by end user population imbalances and normal busy periods for end users, and provide appropriate staff levels to ensure quality of service is maintained.	X		
Perform minor administrative changes to the phone system in order to meet immediate operational requirements.	X		SSC may, on occasion, perform administrative changes to the phone system with consultation from the Service Provider.

End User Service Desk Activities	Service Provider	SSC	SSC Comments
Provide the capacity to increase staffing levels to handle unexpected call volume spikes	X		
Ensure that staffing levels for every shift reflect call volumes patterns.	X		
Adjust phone system open and close hours to reflect statutory holidays to ensure non-business hours script scenarios are followed.		X	
Add new Service Desk Agents phones into the system, or change phone assignments with the addition or movement of Service Desk resources.	X		
Keep the inventory of pre-recorded phone system emergency messages current and accurate.	X		
Record emergency broadcast phone system messages live in both official languages when a message is required and when no appropriate pre-recorded message exists.	X		
Record new phone system wait queues and voice mail messages to reflect any changes in procedure.		X	
Recommend to the Technical Authority changes to the telephony system script or other functions to enhance performance or meet new procedural requirements.	X		
.	X		
Coordinate the implementation and testing of all approved changes with Telecommunications and the vendor.		X	
Run the test script following any change to the system during non-business hours to ensure correct functionality is not adversely affected.		X	
Keep the test script current, complete and accurate.		X	
Report all and any incidents affecting the phone system to Telecommunications immediately upon detection.	X		
Work with Telecommunications and the vendor in order to troubleshoot and rectify incidents to restore service as quickly as possible.		X	During regular business hours, SSC will maintain responsibility for the phone system. After hours, the Service Provider may be

End User Service Desk Activities	Service Provider	SSC	SSC Comments
			asked to provide additional support.
Provide a trusted workaround procedure in the case of an incident affecting the phone system.		X	
Implement trusted workaround procedures until the phone system incident is resolved.	X		
Implement tools necessary to provide Service Desk services and meet SSC informational and functional requirements.		X	
Design, develop, document, and implement manual or backup procedures for Service Desk personnel to follow in the event that the Service Desk tools used to process end user contacts fail to operate properly.	X		
Document escalation procedures to be followed in the event that Service Desk personnel are unable to perform any/part of their job functions because of system, communication, application availability, or other data centre or vendor site related problems.	X		
Establish global work processes for all of the Service Provider's Service Desk installations to deliver consistent Services across locations.		X	
Follow global work processes for all of the Service Provider's Service Desk installations to deliver consistent Services across locations.	X		
Execute availability contingency plans for critical systems when and as required.	X		
Develop and maintain availability contingency plans to ensure that they are kept current, complete and accurate.		X	
Test any and all changes to availability contingency plans as well as participate in regular tests to ensure accuracy.	X		
Report any security breaches such as, but not limited to, reports of viruses to the appropriate authority according to procedure.	X		
Communicate and work with the Security group to remain informed on any security issue.	X		
Provide strategic planning and final direction with respect to both the current services delivered and any services that will be delivered in the future.		X	

End User Service Desk Activities	Service Provider	SSC	SSC Comments
Manage and plan the technologies and associated capacity requirements that will be used in the delivery of services.		X	
Manage the service delivery performance for all delivered services.	X		
Manage the progress, to the extent possible, to a standardized IT environment - infrastructure and architecture.		X	
Manage the quality of the services delivered to each Client.	X		
Manage the Client relationships.		X	
Manage the Contracts and Service Provider relationships.		X	
Service Desk Support			
Record and classify incidents, including priority of request, received from end users and the Service Provider, capturing information and verifying that the Configuration Item (“CI”) information is correct.	X		
Perform a quality assurance review for every call, based on a call back to the end user to confirm satisfaction.	X		
Interact with different levels of IT technical support groups such as to resolve support issues.	X		
Actively monitor all calls, incident, service request problems, and change management tickets for status, and ensure the appropriate action is taken according to procedures and prescribed thresholds.	X		
Actively monitor all tickets for critical high priority incidents.	X		
Validate the end-user's profile or the partner profile to ensure the information is complete and accurate.	X		
Validate that the end-user/partner is entitled to Service Desk Services. The call may have originated at another Service Desk but re-assigned based on the service support.	X		
Capture/record the details for every contact and assess the end-user’s request.	X		
Classify the call according to the available categories and follow the procedures established for the	X		

End User Service Desk Activities	Service Provider	SSC	SSC Comments
category/call type.			
Work with an Automatic Call Distribution telephony system; log in and out, set status, and generate reports as required.	X		
Review classification of incidents throughout their life cycle to elevate to higher priority level as defined by impact and urgency (or as determined by SSC).	X		
Execute incident management in accordance with approved procedures and policies.	X		
Dispatch/route the call to the appropriate Service Desk, service group, or 3rd party vendor if the call cannot be resolved at first point of contact.	X		
Escalate all major incidents.	X		
Track incident and communicate with the end users during the incident life-cycle including confirming resolution.	X		
Identify and communicate problem requests and functionally assign root cause analysis activity to third party vendors.	X		
Conduct Incident troubleshooting and problem determination, for the following areas: network, application, workstation, server, maintenance schedule, I.D. administration (e.g. new logon /account changes), and identification of security incidents.	X		
Check active incident, and problem tickets and associate/link required change tickets to them in order to restore service and perform escalations and notifications to affected stakeholders, as per the SoW.	X		
Establish the criteria for resetting passwords and disclosing them to authorized personnel.		X	
Reset passwords upon first contact.	X		
Action voice mail, email messages and self-ticketing tickets, and respond to them in a timely manner, within the prescribed SLA time frames.	X		
Perform Quality Assurance review ticket resolved by resolver groups outside of EUSD. The QA score must be determined based on 4 call (live or recorded) and ticket evaluations per agent per	X		

End User Service Desk Activities	Service Provider	SSC	SSC Comments
month. The Supplier is responsible for conducting these evaluations. The QA evaluation includes 10 questions covering Customer Service etiquette, procedure adherence, and ticket management.			
Communication and Notification			
Provide status updates to affected end users.	X		Vendor to use SSC approved templates and have any custom messages approved by SSC.
Manage end user communications and notifications on multiple user incidents in accordance with customer communication guidelines and style guides.	X		
Act as a communication centre between the user-client community and the support groups for all workstation requests, incidents and related activities.	X		
Establish and maintain an efficient two-way communication protocol between all support groups related to any aspect of request satisfaction, incident resolution and change to the infrastructure.	X		
Coordinate and organize the dissemination of relevant information to clients.	X		
Participate in a monthly operations review meeting with SSC where all metrics, reports, corrective action statements and recommendations developed by the Service Provider will be reviewed and discussed for SSC approval.	X		
Incident Management			
Incident detection, recording and reporting.	X		
Incident classification and first-line support (e.g. suggestions to solve or workarounds).	X		SSC has the right to re-classify tickets.
Prioritize the incident according to the predetermined Incident Classification and Incident Priority Matrix.	X		
Incident matching between new incident and known incidents, problems or known errors.	X		
Incident investigation and diagnosis.	X		
Incident resolution and recovery.	X		

End User Service Desk Activities	Service Provider	SSC	SSC Comments
Incident closure.	X		
Incident ownership, monitoring, tracking and communication.	X		SSC will provide communications guidelines.
Routing and monitoring of service requests.	X		
Provide technical skills to support applications, maintenance.		X	
Configuration and management of incident management tools.		X	
Problem Management			
Record all relevant details of the potential problem in the Problem Management Service Management Tool following pre-defined processes and procedures.		X	
Co-ordinate problem investigations, conducting root cause analysis, and identifying recurring incidents and identifying problems opening the associated ticket accordingly per pre-defined procedures.		X	
Actively check all problem records for status and priorities.		X	
Actively check all incident records for status and priorities.	X		
Reference the Known Error Database and Problem Management Tool to ensure that no like records already exist prior to flagging a record as a potential Problem.		X	
Follow all pre-defined process and procedures to ensure compliance to the Problem Management Process.		X	
Co-ordinate problem investigations, conduct root cause analysis, and identify recurring incidents and identify problems opening the associated ticket accordingly per pre-defined Problem Management procedures.		X	
Implement pre-defined Problem Management procedures.		X	
Perform quality assurance by reviewing ticket resolution information to ensure that the event is indeed resolved permanently.		X	

End User Service Desk Activities	Service Provider	SSC	SSC Comments
Reference the Known Error Database in order to restore service.	X		

4.3. Request Fulfilment

Request Fulfilment involves the processing of service requests that are defined as pre-approved, low risk changes to the desktop/infrastructure environments that follow standardized and documented procedures. Examples of these types of activities include:

- system account administration
- System resource administration and related activities (i.e. creation and deletion of directories, provisioning of services for mobile devices, etc.)
- assist in any and all security activities as required
- any activity required to deliver services, meet SLAs or SSC service requirements

4.3.1. Request Fulfilment Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Request Fulfilment Activities	Service Provider	SSC	SSC Comments
Account Administration/RFL			
Provide end user administration.	X		
Manage user IDs, create IDs, passwords and end user access as required and authorized.	X		
Co-ordinate and track user ID creation, ID changes and password resets for SSC managed applications.	X		.
Perform directory administration, data moves and removal, creation of distribution lists, new groups, and new shared folders as required according to relevant procedures, ensuring no adverse impact on existing accounts.	X		
Create and/or modify account administration documents, processes and guidelines, modification of processes and guidelines.		X	
Perform Service Desk account security such as obtain accounts, establish accounts, implement accounts, and enforce accounts, as necessary.	X		
Move accounts and associated data between contexts in the network tree and between physical servers in order to ensure the location of the client is reflected in the network tree context and that the load on bandwidth is minimized.	X		

Request Fulfilment Activities	Service Provider	SSC	SSC Comments
Update end user profiles, access groups, shared drives, and distribution groups.	X		
Disable/delete accounts following the approved disabling procedures, including purging deactivated accounts and associated data on a monthly basis.	X		
Obtain/establish, implement and enforce security procedures that will ensure the safety of the corporate and individual's information for all accounts processed by the EUSD.	X		
Manage, prevent, resolve and report account administration integrity issues.	X		
Assist end users in the addition, creation and changes of logon IDs according to SSC defined processes for access requests.	X		
Create new logon IDs, file shares and appropriate directories.	X		
Set up end users with standard site logon configuration files.	X		
Perform end user ID deletes including removing IDs and delete, file share and permission management, archive or move associated data to a new owner.	X		
Make logon ID changes in user privileges as requested via SSC defined access request process.	X		
Request Fulfilment (RFL) and Change (RFC)			
Validate the request and ensure the proper information and approvals have been obtained from the Client Representative.	X		
Perform checking of the necessary IT environment for change management such as requests for change and account administration aspects to ensure client service is uninterrupted.	X		
Initiate change management tasks such as validation of requests, determine and tailor requests, task, workflow quality assure, close requests, report.	X		
Modify group shared folders and group accesses for Novell.	X		
Record all details of the request per pre-defined templates.	X		

Request Fulfilment Activities	Service Provider	SSC	SSC Comments
Classify the RFC and determine the change model.	X		
Assign the RFC to the appropriate service groups.	X		
Monitor the RFCs requesting status updates and updating the request.	X		
Perform required escalation per the pre-defined process and procedures.	X		
Modify task flows.		X	
Inform appropriate support groups of issues related to a change request, and escalate any issues to the relevant group(s).	X		
Ensure work performed is accounted for and required action are taken to respect the request.	X		

4.4. Transition Services

The transitions in (from the current Service Provider) and out (to any future Service Provider) must be accomplished in a manner that is non-disruptive and well planned to accommodate the progressive takeover of the service delivery. The transition processes must minimize risk to the quality of service, and cause minimal impact to clients' operations.

4.4.1. Transition-In Plan

Within 14 calendar days of the Contract Award Date, the date of issuance of the Contract by SSC, the Service Provider must provide to SSC a Transition-In Plan ("TIP") for approval and acceptance. It must be sufficiently detailed to clearly identify how the Service Provider will transition-in all of the End User Service Desk and Request Fulfilment services from the current Service Provider. At a minimum, the TIP must include, but is not limited to:

- How the Service Provider will obtain an understanding of the entire Service Desk and Request Fulfilment Domains and all functions and sub-functions contained within
- How the Service Provider will staff, train and prepare their workforce so that they are fully capable of providing services (i.e. Resource Plan)
- Identification of the key resource names and security classifications so site security accesses can be pre-arranged and the beginning of the submission of the résumés for the remaining key resources who will make up the total key resources to be working at the start of Transition-In activities
- EUSD and RFL knowledge transfer strategy for all key resources and for all Service Provider resources;
- Service Provider's proposed transition schedule
- Training plans and methodology (which would include but not be limited to: shadowing with outgoing contractors, site visits, familiarization with tools, study of SSC-provided operational documentation and internal assessment methodology)
- How the Service Provider will obtain an understanding of the EUSD and RFL technical environments, support structure and business relationships; and

- Reporting strategy including:
    - Weekly Transition-In Reports (including but not limited to attainment levels per training category and resource levels);
    - Weekly Operational Reports, as described in Appendix A to Annex A
    - Establishing service level reporting, as described in Appendix A to Annex A
    - Establishing quality reporting, as described in Appendix A to Annex A
    - Transition-in incident reporting; reporting (including but not limited to Daily Backlog Report and Activity Plan as described in Appendix A to Annex A
    - Service Provider-related escalation process/governance

The 30 calendar days immediately following the date of acceptance of the TIP is the Transition-In Period, during which the TIP must be implemented by the Service Provider. SSC will not change the technical infrastructures or environments identified in the RFP during the Transition-In Period. The Transition exercise is of critical importance to ensure that the Service Provider is fully capable of performing the responsibilities of the Function at Contract Start Date and to demonstrate to SSC that the expected levels of service are being achieved.

On the day after the date of acceptance of the TIP, the Service Provider must provide, on site, the Resources outlined in task authorization in accordance with Appendix C to Annex A – Tasking procedures, in the event that the resource proposed in the Service Provider's Proposal is unavailable through no fault of the Service Provider, a substitute approved and accepted by SSC. This substitute must meet all of the requirements associated with the category as per Appendix D to Annex A – Resource Assessment and Criteria response tables, meet the language requirement relative to the ratios identified in Section 2.4, and hold a valid security clearance at the requisite level to be accepted.

SSC will ensure that the documentation maintained by the incumbent Service Provider will be complete, approved by SSC, and available for use by the new Service Provider upon contract award.

The Transition-In must be completed by the Service Provider within 30 calendar days following the date of acceptance of the Transition-In Plan [the "transition" – in TIP]. The Contract Start Date is the day immediately following completion of the 30-day Transition-In. At the Contract Start Date the following must have occurred:

a) The functions must be transitioned to new Service Provider
b) The key resources must be autonomous in their new roles
c) The Service Provider must have provided the minimum staffing requirement of key resources as identified, or their equivalent as approved by SSC
d) The Service Provider must have taken full responsibility for the delivery of all functions.

SSC will pay the Service Provider as per the Request for Proposal if all of (a) through (d) above have occurred.

4.4.1.1. Transition-In Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Transition-In Activities	Service Provider	SSC	SSC Comments
Transition-In			
SSC will not change the technical infrastructures or environments during the 30-day Transition-In Period.		X	

Transition-In Activities	Service Provider	SSC	SSC Comments
Ensure key resources are available on a full time basis from the first day of the Transition-In Period, and for a minimum of 6 months following the end of the Transition-In Period.	X		
Ensure key resources are available to perform certain work outside of regular business hours as required.	X		
Key resources must be made available as required by SSC, and will be expected to learn the key aspects of the functions from the incumbent resources during the Transition Period.	X		
Key resources must transfer this knowledge to the winning bidder's remaining contractor resources by the Contract Start Date.	X		
The resources proposed by the winning bidder must have the experience, skills and knowledge to perform their roles, and may require specific knowledge transfer on specific aspects of the SSC domain or systems to assume operational responsibilities.	X		
Service Provider must ensure that resource availability is maintained and that the Service Provider's Transition activities do not cause service disruptions.	X		
If an equivalent resource is provided, the resource is subject to approval by SSC.	X		
Service Provider must provide to the a weekly "Transition-In" report detailing the status of all "Transition-In" activities as well as transition issues, mitigation, progress, recommendations and any other pertinent details.	X		
All requirements of the Transition-In Plan must be implemented on schedule.	X		
Service Provider must carry out the transition of its staff and processes associated with a function such that it is ready and able to carry out all work associated with the function by the end of the Transition-In Period.	X		
The Transition exercise is of critical importance, to ensure that the Service Provider is fully capable of performing the responsibilities of the function and to demonstrate to SSC that the expected levels of service are being achieved.	X		

Transition-In Activities	Service Provider	SSC	SSC Comments
SSC shall notify the Service Provider, in writing, of acceptance of the Transition when the Service Provider has demonstrated to the satisfaction of SSC that it is ready to carry out all of the work described in this SOW.		X	
All costs associated with the Transition shall be the responsibility of the Service Provider.	X		

4.4.2. Transition-Out Plan

At the end of the Contract Period, the Service Provider must assist with the transition of the Domain to a new Service Provider. The Service Provider must cooperate with a new Service Provider to ensure that smooth and seamless transition of services occurs. The Service Provider must ensure that overall operational availability is not disrupted; existing service levels are maintained and Contract deliverables continue to be delivered while transition and knowledge transfer to a new Service Provider occurs.

4.4.2.1. Transition-Out Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Transition-In Activities	Service Provider	SSC	SSC Comments
Transition-Out			
Ensure that all documentation (i.e. operational, training, reporting, etc.) Is up to date and accurate. Copies of all documentation must be provided within 2 working days on written request from SSC.	X		
Ensure operational procedures are up to date and accurate.	X		
Ensure operational checklists are maintained to current requirements and are complete and accurate. Copies of these checklists must be provided within 2 business days on written request from SSC.	X		
Continue to meet established operational service levels and targets.	X		
Continue to meet existing service level targets as they relate to Incident Management, Change Management, and Request Fulfillment.	X		
Allocate the necessary time to assist in one-on-one knowledge transfer to the incoming Service Provider.	X		

Transition-In Activities	Service Provider	SSC	SSC Comments
Prepare and deliver detailed transition documentation for presentation to SSC to be utilized with the incoming Service Provider. The transition documentation and presentations must be provided for each function and sub-function within the Request for Proposal. The documentation must describe, in the necessary detail, all the pertinent and important details necessary for a successful transition to the incoming Service Provider.	X		
Prepare weekly Transition-Out reports.	X		

5. Resource Requirements

This section details the resource requirements required to perform the functions within the End User Service Desk.

5.1. Expected Quality

The expected annual volume of calls for the End User Service Desk is approximately 302,000. The expected annual volume of requests for Request Fulfilment is approximately 64,200. These volumes will need to be processed as per the SLAs using the resource numbers listed in section 5.2.

5.2. Resource Positions

Service	Function	Position Title	Qty
EUSD	Domain Management	Service Delivery Manager	1
EUSD	Domain Management	Domain Team Lead	1
EUSD	Domain Management	Reporting Analyst	2
EUSD	Domain Management	Quality Analyst	1
EUSD	Domain Management	Client Delivery Executive	.5
EUSD	Incident Management	Senior Service Desk Agent	5
EUSD	Incident Management	Team Lead	2
EUSD	Call Management	Intermediate Service Desk Agent	43
EUSD	Call Management	Junior Service Desk Agent	17
RFL	Request Fulfillment	Senior Account Administrator	3
RFL	Request Fulfillment	Intermediate Account Administrator	13
RFL	Request Fulfillment	Junior Service Order Agent	2
RFL	Request Fulfillment	Flow Controller	1
RFL	Request Fulfillment	Team Lead	1

5.3. Position Descriptions

Domain Management

Service Delivery Manager

The Domain Management Service Delivery Manager ("SDM") manages the daily operations of the operations and coordination staff. They are the single point of contact for day to day service delivery, and ensure performance and quality of service is met.
Domain Management SDM must meet the following requirements

- 7 years of experience in the management of IM/IT service desks, teams, budgets and contracts in a Government or large corporate environment of 5,000 or more end users
- 7 years of experience producing and implementing comprehensive Monthly Action Plans ("MAP") for Service Desk optimization such as:
    - SD metrics
    - implementation of SD process improvements
    - training gaps
    - client service expectations
- 7 years of ' experience defining technical specification workload estimates in relation to SD services
- 7 years of experience ensuring that the Service Level Targets are met and that those missed are documented
- 7 years of experience in monitoring and testing contingency plans for critical Service Desk systems
- 7 years of 'experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf (COTS) office products such as MS Office. Technical support can include such as password resets, hardware issues related to damaged peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware security incidents such as viruses and malware
- 7 years providing expertise and guidance with regards to a Service Desk environment for Service Desk functions related to workstations, server and client environments
- 7 years of experience implementing corrective actions in a call centre environment related to call, incident, problem and change management and escalation processes
- 7 years of experience reviewing service management status reports including data related to quality assurance, daily and weekly call statistics, issue/problem resolutions
- 7 years of experience in the analysis of IT Service Desk workload reporting to determine process improvements in areas such as call resolution, customer service
- Valid Federal Government Level II Secret Security Level Clearance

5.2.1.2 Domain Team Lead

The Domain Team Lead is a Supervisor, managing employees and overseeing operation of the Service Desk.
Domain Team Lead must meet the following requirements

- 5 years' experience providing Information Technology technical support services in client operating systems, networks operating software, or commercial-off the-shelf ("COTS") office products (MS Office). Technical support can include such as password resets, hardware issues related to damaged peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware

- 5 years' experience in the management of IT projects and teams
- 5 years' experience implementing Management Action Plans ("MAP") in a Service Desk environment such as:
    - SD metrics
    - implementation of SD process improvements
    - client service expectations
- 5 years providing expertise and guidance with regards to a Service Desk environment for Service Desk functions related to workstations, server and client environments
- 5 years' experience implementing corrective actions in a call centre environment related to call, incident, problem and change management and escalation processes
- 5 years' experience determining technical workload specifications in relation to the Service Desk environment
- 5 years' experience reviewing service management status reports including data such as quality assurance, daily and weekly call statistics, issue/problem resolutions
- 5 years' experience in the analysis of IT Service Desk workload reporting to determine process improvements in areas such as call resolution, customer service
- 5 years' experience in the provision of IT support client services within an IT environment for a Government or large corporate environment of 5,000 or more end users
- Valid Federal Government Level II Secret Security Level Clearance

Reporting Analyst

The Domain Reporting Analyst gathers and performs analysis on statistical data. They then use this to generate reports on Service Desk performance.
Domain Reporting Analyst must meet the following requirements

- 4 years' experience producing reports for a Service Desk environment such as overall expertise, knowledge and performance levels for each specific area of expertise, such as Service Desk Agents ("SDA") for call, incident, problem, change, as well as Account Administrator ("AA"), Task Flow Controller ("TFC") and change requests
- 4 years' experience in the use of spreadsheets for tracking workload metrics on calls, incidents, problems and changes on a daily, weekly, monthly and quarterly basis
- 4 years' experience in tracking of metrics related to a Service Desk environment such as metrics and volumetric that demonstrate optimal performance of Problem resolution and request processing
- 4 years' experience producing documentation related to collection of metrics such as weekly activity statistics, call metrics, service management metrics, monthly resource requirements based on workload, SLA obligations
- Valid Federal Government Level II Secret Security Level Clearance

Quality Analyst

The Domain Quality Analyst is responsible for reviewing the quality of a percentage of tickets, and providing feedback to the agent.
Quality Analyst must meet the following requirements

- 4 years' experience in providing quality assurance in a Service Desk environment in preparing things like quarterly reports on findings, deficiencies, degradation, problems with existing processes, procedures, Service Desk Agents and recommended corrective measures and/or improvements

- 4 years' experience with an enterprise class IT Service Management record, prioritize, match against other tickets in the system , track, document, assign and close call/incident, problem and IMAC/change tickets
- 4 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required
- 4 years' experience in the analysis of quality assurance data related to a Service Desk environment such as the effectiveness and performance of all service desk tasks
- 4 years' experience in the use of spreadsheets for quarterly samples tickets (calls taken and problem number assigned) and reports detailing Service Desk Agent resolution rates of problems
- 4 years' experience in tracking of quarterly samples tickets (calls taken and problem number assigned) and reports on the Service Desk's quality of Service Requests
- 4 years' experience producing reports for a Service Desk environment such as on the integrity and day-to-day procedures of the SD indicating where the quality of work has degraded, maintained, or improved
- 4 years' experience producing documentation related to collection of metrics such as problem resolutions and request processing
- Valid Federal Government Level II Secret Security Level Clearance

Client Delivery Executive

The Client Delivery Executive oversees the delivery of the contract.
Client Delivery Executive must meet the following requirements

- 10 years' experience in developing and monitoring of Service Desk action plans, policies, and guidelines
- 10 years' experience in the analysis and engineering of Information Technology processes to optimize operations
- 10 years' experience in analysis of Service Desk reports to ensure client service objectives are met such as overall satisfaction and service levels are being met and to address Service Desk delivery issues
- 10 years' experience in customer relationship management with government departments or large private sector organizations with over 5,000 resources
- 7 Project Management experiences and valid certification
- Valid Federal Government Level II Secret Security Level Clearance

Incident Management

Senior Service Desk Agent

The Incident Management Senior Service Desk Agent ("SDA") is an experienced resource acting as a point of contact for internal escalation related to issues that Service Desk Agents are unable to resolve. They are also specialized in processes and procedures in a specific stream.
Senior Service Desk Agent must meet the following requirements

- 4 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close Service Request l/incident, problem and IMAC/change tickets
- 4 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf (COTS) office products Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as

non-responding applications, identification of security incidents such as viruses and malware

- 4 years' experience working with an Automatic Call Distribution telephony system log in and out, set status, generate reports as required
- 4 years' experience providing coaching/mentoring to team members in an IT environment
- Valid Federal Government Level II Secret, or Enhanced Security Level Clearance

Team Lead

The Incident Management Team Lead provides direction, instructions, coaching and guidance to a group of individuals.
Team Lead must meet the following requirements

- 5 years' experience working with an enterprise class IT Service Management tool, record, prioritize, match against other tickets in the system , track, document, assign and close Service Request l/incident, problem and IMAC/change tickets
- 5 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products. Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware of security incidents such as viruses and malware
- 5 years' experience interacting with different levels of IT technical support groups such as to resolve support issues, participate in projects
- 5 years leading a team of professionals in the delivery of IT services such as:
  - call management
  - on-line support
  - problem and incident management
  - escalation
- 5 years' experience in the documentation of technical IT solutions
- 5 years' experience providing coaching to IT clients and team members
- Valid Federal Government Level II Secret Security Level Clearance

Call Management

Intermediate Service Desk Agent

The Intermediate Service Desk Agent ("SDA") answers calls, performs basic troubleshooting and attempts first call resolution.
Intermediate Service Desk Agent must meet the following requirements

- 3 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf (COTS) office products. Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware
- 3 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close service request l/incident, problem and change tickets
- 3 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required
- Valid Federal Government Level II Secret, or Enhanced Security Level Clearance

Junior Service Desk Agent

The Junior Service Desk Agent ("SDA") is responsible for answering simple Level 1 calls and attempting first-call resolution. Examples of this type of call would be a password reset or an account unlock.
Junior SDA must meet the following requirements

- 2 year experience or an acceptable combination of education, training, and/or experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products Technical support can include password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware
- 2 year experience OR an acceptable combination of education, training, and/or experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close service Request l/incident, problem and/change tickets
- 2 year experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required
- Valid Federal Government Level II Secret, or Enhanced Security Level Clearance

Request Fulfillment

Senior Account Administrator

The Senior Account Administrator is an experienced resource acting as a point of contact for escalations related to issues that Account Administrators are unable to resolve. They are also knowledgeable in processes and procedures for a given stream.
Senior Account Administrator must meet the following requirements:

- 4 years' experience providing technical support in an IT environment
- 4 years' experience in providing account administration services in Microsoft Active Directory
- 4 years' experience working with an enterprise-class IT Service Management tool
- Valid Federal Government Level II Secret Level Clearance

Intermediate Account Administrator

The Intermediate Account Administrator is responsible for performing complex account administration tasks and system maintenance as well as resolving incidents resulting from activities previously performed.
Intermediate Account Administrator must meet the following requirements:

- 3 years' experience providing technical support in an IT environment
- 3 years' experience providing account administration services in Microsoft Active Directory
- 3 years' experience working with an enterprise-class IT Service Management tool
- Valid Federal Government Level II Secret, or Enhanced Security Level Clearance

Junior Service Order Agent

The Junior Service Order Agent is responsible for performing simple account administration tasks as well as monitoring changes in the environment that have been submitted to request service or may impact account administration activities.

Junior Service Order Agent must meet the following requirements:

- 2 year experience OR an acceptable combination of education, training, and/or experience providing technical support in an IT environment
- 2 year OR an acceptable combination of education, training, and/or experience providing account administration services in Microsoft Active Directory
- 2 year experience working with an enterprise-class IT Service Management tool
- Valid Federal Government Level II Secret, or Enhanced Security Level Clearance

Flow Controller

The Flow Controller is responsible for performing routing of incidents and IMAC (Install, Move, Add, and Change) requests to available administrators for processing or resolution.

Flow Controller must meet the following requirements:

- 3 years' experience providing technical support in an IT environment
- 3 years' experience working with an enterprise-class IT Service Management Tool

Team Lead

The Request Fulfillment Team Lead provides direction, instructions, and guidance to a group of individuals.

Team Lead must meet the following requirements:

- 5 years' experience providing technical support in an IT environment
- 5 years' experience providing account administration services in Microsoft Active Directory
- 5 years' experience working with an enterprise-class IT Service Management tool
- 5 years leading a team of professionals in the delivery of IT services
- 5 years' experience providing coaching to clients and team members
- Valid Federal Government Level II Secret Level Clearance

PART 2
SSC ENTERPRISE SERVICE DESK

1. Introduction
The scopes of the Services that are the subject of this RFP are detailed in Section 4 of this document, and include the following:

- Service Management Functions (see Section 4.1 for more details);
- Enterprise Service Desk ("ESD") (see Section 4.2 for more details);
- Transition Services (see Section 4.4 for more details).

Shared Services Canada ("SSC") has written the service descriptions to focus on specific outcomes and activities the Service Provider must execute.

2. Contract Terms

b. Location

All services will, initially, need to be delivered from the National Capital Region (NCR). .

In the event of a disaster at the present location of operations, the Service Desk shall be reassigned to a Disaster Recovery ("DR") site within the NCR to resume operations until the situation is rectified, as per current SSC Business Continuity procedures.
It is expected that all resources will be centrally located in the NCR SSC will provide the Service Provider with sufficient notice of any facility (or service delivery location) changes. Changes to the location will not trigger a change to pricing or other expenses. Bidders are expected to take this into consideration in their pricing responses.

c. Workstations and Telephones

During the Contract period, SSC will provide workstations for the Service Provider's resources to use. The Service Provider will also be provided with an office phone system that includes Service Desk Agent phones. Bidders are encouraged to review the Financial Responsibility Matrix tab in the Pricing Template Attachment 3.1 for clarity on what SSC will provide and what the Service Provider is responsible for providing in their pricing submission.
The Service Provider must provide its resources with smart phones as required at their own expense.

d. Operating Hours

Enterprise Service Desk Services must be provided on a 24 hours a day, 7 days a week, and 365 days a year including all holidays. There are some activities that are not required to be delivered on a 24 x7 basis and those can be delivered during the Government of Canada core business hours which are (07:00 to 17:00) Monday to Friday excluding federal statutory holidays.

e. Language Requirements

All Enterprise Service Desk agents and management staff must be bilingual in English and French. 75% of the Request Fulfillment staffs are required to be bilingual in English and French.

f. Security Clearance Requirements

All Enterprise Service Desk management staff resources must obtain Level II Secret Government of Canada security clearance and maintain Level II Secret security clearance for the duration of their employment. SSC will temporarily allow Service Provider staff to provide services as long as they have received Reliability Status and have submitted an application for Level II Secret clearance. No less than 80% of the Service Provider staff delivering the services must have their Level II Secret clearance.

3. Current State Summary

Since 2013, SSC has outsourced their Enterprise Service Desk function to an existing Service Provider. The contract with this Service Provider is set to expire on June 30th 2018. All SSC and Government of Canada data currently resides in Canada and this mandatory requirement must be maintained throughout the duration of the subsequent contract.

b. Enterprise Service Desk

The Enterprise Service Desk ("ESD") uses a desk to desk model. The ESD is the first point of contact for all customer Service Desks. The service includes the fulfilment of service requests as well as incident management which includes ticket creation, escalation, and resolution wherever possible.

The Enterprise Service Desk currently provides services for the 43 customers of Shared Services Canada, as well as other client departments/agencies of the Government of Canada, on a 24 hours a day, 7 days a week basis. It serves as the national escalation point of contact for all tickets from the various partner and department service desks. The ESD is also the interface to third-party vendors and operates as the after-hour partner and department service desk responsible for incident creation, escalation, and resolution.

Currently the primary contact methods are toll-free number, email and an on-line portal with the potential of expanding to other contact channels as technologies become available.

1. Telephony

The current Service Desk telephony solution is a hosted Centrex solution provided by a third-party and accessed via the Internet. End users call a main number (specific to their organization) that is forwarded to a Control Directory Number ("CDN"). The Automated Call Distribution ("ACD") system is then controlled by client software running on a workstation communicating with the hosted solution. The Service Provider has access to monitoring and administration tools with capabilities such as, but not limited to: Registration of agents, designation of skill sets, recording and loading of broadcast messages, production of reports and monitoring of live call activity are performed from this console. Future capabilities for call recording and skill based routing will become available in 2018.

2. Remote Takeover Tools

Currently, the remote takeover tools used by the Service Desk are SCCM Client Centre and Cisco WebEx Support Centre. These tools are available to connect to virtually every end-user's production networked workstation. It is expected that all agents are trained to use these tools to ensure high First Contact Resolution service levels are achieved when possible. The tools used for remote takeover are subject to change at SSC's discretion.

3. Knowledge Base

Get Answers, GCdoc, and ECD are the current Enterprise Service Desk's knowledge base tools. Articles are kept current as new applications, end-users, or products are added to the environment. The ESD knowledge base contains common Process and Procedure with the plan to leverage the tool to also include incidents with their solutions as well as recommended resolutions for common incident symptoms. It is expected that all agents are trained to use the ESD knowledge base to ensure high First Contact resolution service levels are achieved. The Service Provider must also contribute new articles and recommend changes to existing articles to keep the ESD knowledge base current. The ESD knowledge base tools are subject to change at SSC's discretion.

4. Incident and Change Management Tools

Multiple ITSM tools are used in supporting all of SSC's customers, such as InfoMan/InfoWeb, Enterprise Control Desk (ECD), HP Service Manager, and TCassist (SMGS). The ITSM tools in use are subject to change at SSC's discretion.

4. Service Descriptions

This section details the service requirements the Proponents will be expected to include in their Proposal and pricing. These services do not necessarily reflect what or how services are currently delivered by the Current Service Providers.

b. Service Management Functions

Service Management Functions Services are activities that the Service Provider must perform across all functional areas.

Where there is an impact or interaction with SSC, the Service Provider is expected to deliver the Services using industry standard methodologies and market best practices. SSC may request documentation that provides proof of this. The Service Provider will be expected to follow relevant SSC policies and procedures.

1. Governance

The objective of Governance is to:

- monitor and ensure consistent quality for services being delivered to SSC by the Service Provider;
- proactively identify, assess and mitigate risks (both operational and reputational) to SSC stakeholders and ensure compliance to SSC policy and procedures;
- ensure interpretation and compliance to the contract and changes to the terms of the contract and/or SLAs;
- monitor and ensure consistent strategic alignment between stakeholder strategies and service requirements to the Service Provider performance;
- develop, implement, and manage processes such as call, incident, event, problem, change, service request, and management;
- ensure appropriate levels of engagement between internal stakeholders and the Service Provider at the right point in time in the governance processes;
- provide central reporting and proactively identify areas of improvement;
- provide a continuous improvement framework which strengthens operational performance and fosters the development and implementation of technologies that are in line with technology standards and industry best practice;

1. Governance Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Governance Activities	Service Provider	SSC	SSC Comments
ESD Management			
Lead a team of professionals in the delivery of IT services such as overseeing workforce management, quality assurance and operational performance.	X		
Provide coaching to team members.	X		
Implement approved management processes.	X		
Establish mechanisms for ongoing working interfaces (e.g. daily, weekly or monthly meetings and quarterly reviews) with team members managed under the Service Desk contract as well as contractors associated with other contracts.	X		
Manage all personnel based resources in such a manner to avoid any master-servant relationship with respect to SSC and the contractor's personnel resources.	X		
Establish the necessary management structure and related processes to ensure that all responsibilities that are specified in this SOW are carried out such that the terms and conditions are met.	X		
Participate in and lead projects as required.	X		
Liaise with various work units and personnel to determine resource requirements as necessary to complete project work.	X		
Manage projects to ensure that milestones are met in accordance with project guidelines.	X		
Provide a mechanism to track agent utilization for those personnel's who do not use a system that tracks agent state and/or time allocation.	X		
Plan, manage and execute all contracted activities.	X		
Identify, define and report on workload metrics that best measure the performance of all personnel and the overall operation.	X		
Develop and implement comprehensive Monthly Action Plans ("MAP") that identify how performance and quality issues that must be resolved.	X		
Provide expertise and guidance with regards to overseeing operations providing Service Desk	X		

Governance Activities	Service Provider	SSC	SSC Comments
support			
Implement corrective actions or process improvements related to call, incident, problem, escalation and change management.	X		
Determine technical workload specifications (i.e. staffing levels) in relation to the Service Desk environment.	X		
Review service management performance reports such as quality assurance, daily and weekly call statistics, and issue/problem resolutions.	X		
Analyze Service management performance reports to determine corrective actions and process improvements in areas such as call resolution, customer service.	X		
Liaise with various work units and personnel to address issues directly affecting day-to-day operations.	X		
Work with various work units and personnel to define appropriate paths for the flow of contract information and status.	X		
Provide 24 hours per day, 7 days a week, 365 days per year, a mechanism for all Service Desk personnel to call another resource for help and guidance prior to escalating to on-call resources.	X		
Provide 24 hours per day, 7 days a week, 365 days a year, a mechanism for the on-call resources to escalate issues.	X		
Create and update all existing and required functional and operational documentation and procedures to ensure that they are kept in an accurate, current, and complete state at all times	X		
Review all service requests as well as categories and statuses used by the Service Desk, and recommend changes to ensure that the categories and status reflects at all times the nature and the flow of work processed.	X		
Train Service Desk staff according to SSC's approved training plan and curriculum. Demonstrate that effective and successful training occurred.	X		At Service Provider's expense
Update and maximize the use of automated alerts, e-mails, processes and procedures in use within the	X		

Governance Activities	Service Provider	SSC	SSC Comments
Service Desk.			
Maintain or improve the ESD's knowledge base accuracy and effectiveness.	X		
Recommend functional and informational changes to the ITSM tool in order to improve overall use of the ITSM tool and performance of the Service Desk and the information passed on to support groups.	X		
Develop and implement performance monitoring processes to ensure quality service is provided and productivity targets are met or exceeded.	X		
Work with the performance measurement group and incident management group in the processing and management of Customer satisfaction surveys or feedback.		X	
Review client satisfaction surveys and customer feedback to take corrective action (i.e. update documentation, address performance concern, callback customer, etc.) in response to unsatisfactory feedback.	X		
Make resources available, at any time of the day and the week, to work with the technical authority to restore regular service in case of major system and environmental problems, such as: natural disaster, virus, etc.	X		
Attend all daily and weekly service management meetings, such as the "what happened yesterday" (WHY) meetings, and provide all required status and reports in order to meet process and service management requirements.	X		
Oversee Service Desk personnel training, mentoring and coaching to ensure compliance with performance standards for: x. call etiquette xi. system access xii. creating and closing (tickets) xiii. linking call records to tickets xiv. referencing change requests xv. escalation procedures xvi. password reset xvii. contingency plans xviii. standard Service Desk procedures xix. ESD knowledge base management and known error database	X		

Governance Activities	Service Provider	SSC	SSC Comments
Evaluate personnel and position them where they will be most effective to meet service level targets as per the SoW.	X		
Test and execute contingency plans for critical Service Desk functions and systems.	X		
Act as a central point of contact to provide technical information such as the nature of the incident, status, technical specifications, needed for additional information between the user-client community and the IT support groups, for all requests, incidents and related activities.	X		
Ensure that Service Desk procedures are kept current in accordance with operational directives.	X		
Monitor missed service levels to ensure performance improves.	X		

2. Reporting

The Service Provider performing any of the Service Desk Functions and Sub-Functions must develop, deliver and maintain a system and processes for specific Workload Metrics (WM) to: collect, store, query and report information that identifies and measures the volume, quality and service level of work performed and the resources required to perform work associated with that Service Desk Function and/or Sub-Function. This Workload Metrics System (WMS), including associated reports, will provide SSC with the necessary information to fully monitor operations.

Within the first 3 months following the Contract Start Date, the Service Provider must provide to SSC, its proposed WMS, including sample reports that will use specific Workload Metrics. SSC retains the right to request further development, changes and further reports from the Service Provider to be included in the WMS. SSC's approval of the WMS will be provided through written communication. The WMS and reports must be prepared and submitted to SSC every calendar month, as described below, or within 5 business days upon written notice by SSC.

At any time, SSC is entitled to access and audit any Workload Metric and Performance Measurement reports and systems for completeness, accuracy and content. Complete lists of reports are defined in Appendix A to Annex A Reporting Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Reporting Activities	Service Provider	SSC	SSC Comments
Design, develop, maintain and deliver Service Desk reports on SLA and KPI's requested by SSC.	X		
Provide reporting analysts to address periodic ad hoc reporting requests regarding user contacts and SSC information, to be approved by authorized SSC personnel.	X		

Reporting Activities	Service Provider	SSC	SSC Comments
Provide access to raw data captured within the service management tool for consumption and manipulation by customer analysts and management.	X		
Track and report workload metrics on calls, incidents, events, problems and changes on a daily, weekly, monthly and quarterly basis.	X		
Report weekly on all activities at the Service Desk including, but not limited to, call metrics and service management metrics such as call, incident and change management tickets.	X		
Review daily tickets for quality and compliance to documentation standards and administrative processing protocols.	X		
Explain and demonstrate monthly the human resource usage based on workload and metrics. l. Report monthly on the resource requirement for each process based on workload. Demonstrate and report that quality thresholds for each indicator for each process are met.	X		
Report monthly on overall expertise, knowledge and performance levels for each specific areas of expertise such as junior, intermediate and senior Service Desk agents and coordinators for call, incident, problem, change, as well as intermediate and senior account administrators.	X		
Report monthly on general performance relative to SLAs' obligations and objectives, (i.e. met or not met, or the proportion of time taken).	X		
Report quarterly on the integrity and day-to-day procedures reviewed, indicating where the quality of work has degraded, maintained, or improved. Perform regular reviews of the day-to-day procedures that may lead to errors, account duplication, account not in appropriate context, or inactive.	X		
Report weekly on all incidents resolved and not resolved at the Service Desk. Perform quality assurance (exercise quarterly and report on findings, deficiencies, degradation, and problems with existing processes, procedures, staff and recommend corrective measures and/or any improvements).	X		
Produce monthly metrics and volumetric that	X		

Reporting Activities	Service Provider	SSC	SSC Comments
demonstrates optimal performance or any required improvement in performance relating to incident resolution and request processing.			
Report weekly on all service requests.	X		
Report quarterly on recommendations on ways to improve handling of service requests.	X		

c. Enterprise Service Desk ("ESD")

The objectives of the Enterprise Service Desk are to:

- Operate and maintain a Service Desk 24 hours a day, 7 days per week, to ensure prompt and quality infrastructure environment support to multiple customer departments and service desks;
- Act as a single point of contact for all requests and resolve issues on first call or route to the appropriate resolving service line (support group) or vendor;
- Perform active case management, be accountable for end to end delivery of requests and ensure resolution is driven by all downstream service lines (support groups);
- Function as the incident Management lead to coordinate the resolution of all incidents;
- Meet SSC's service level objectives:
    - Average Speed to Answer is 70% <120 seconds and 90% <300 seconds
    - Abandon Rate is <7.5%
    - Response time for Email request within 4 hours
    - Response time for Self-Service request within 4 hours
    - Response time to Email listener ticket within 1 days

The Service Provider must provide Service Desk services consistent with an industry leading operation. The Service Provider must create or update a ticket for every request or reported incident and be responsible for updating and managing the ticket throughout its entire lifecycle. SSC will need visibility at all times to the status of tickets so they can be informed and capable of responding to questions from SSC staff.

Incidents will be reported directly to the Service Desk by phone, email or through online interfaces (i.e. portal) which automatically create a ticket in the ticketing system. It will be the Service Provider's responsibility to resolve incidents on first contact and, if the incident or request will be escalated, gather sufficient information to share with the service lines (support groups) or vendors. The Service Provider must perform due diligence to discover, understand and integrate with the current escalation processes between the various support teams in SSC.

SSC will provide the facilities, office equipment, voice equipment and network connectivity for the delivery of Enterprise Service Desk services as defined in the Attachment 3.1 - Pricing Submission Sheet.

To reduce the number of Service Desk contacts, SSC provides users the ability to resolve problems on their own. The Service Provider must proactively document solutions to common problems and, in the future, SSC will post to the SSC self-service portal where users may search for common solutions.

Upon receipt of an incident from an SSC employee, authorized SSC representative or from an alert from a monitoring system, the Enterprise Service Desk must log the incident in the ticketing system

and perform an initial investigation to resolve the incident or dispatch to the appropriate support team. This will require the Service Provider to initiate hierarchic escalation within SSC and the Service Provider's organization to provide the appropriate management communications when a critical incident occurs. The resolver may be an SSC service line (support group), a Service Provider support group or a vendor. SSC is responsible for procuring and maintaining all necessary contracts with Third Party vendors for which they have a direct relationship, for providing the Service Provider with all necessary vendor contact and contract information and identifying the appropriate queue within the Ticketing System for incidents that are to be resolved by any specific SSC service line or vendor.

If the Service Provider is unable to resolve an incident upon its initial investigation, the Service Provider will route the ticket to the appropriate support team. The Service Provider will contact the appropriate support team, in the case of incidents related to the system or any services provided by Service Provider, or the appropriate SSC or Third Party resolver in the case of all other incidents.

SSC reserves the right to change the classification/priority/severity in cases where SSC determines the business or end-user impact is higher than initially determined by the Service Provider.

The Service Provider must perform incident analysis and diagnostics to determine the cause of the reported incident. The Service Provider must also perform ticket monitoring, re-assignment, escalation and notification of High priority tickets and/or service level issues, as well as Technical and Performance Analysis. The Service Provider must track and report on how much time was spent working on each ticket across each stage of the technical support lifecycle (e.g., Diagnosis, Resolution, etc.).

The Service Provider must provide remote support to devices which includes (but not limited to) servers, as well as Smartphone support limited to email service related tickets consistent with industry leading processes and frameworks. The Service Provider will be required to coordinate and work with support staff to ensure requests are fulfilled and tickets are resolved. The Service Provider will be responsible for dispatching and assigning tickets to support staff and verifying all activities have been completed.

1. Incident Management

For further clarification, the Service Provider is responsible for incident management for all clients of the Enterprise Service Desk. The Service Provider must designate an on-duty incident coordinator with the responsibility for coordinating responses to significant incidents that involve outages and/or performance degradation with the Service Provider, SSC, and other Third Parties as needed. This resource must act as the primary contact between SSC and the Service Provider for resolution of these incidents.

SSC will require the Service Provider to document, report, and coordinate the resolution of all incidents. This requires the Service Provider to isolate the incident, document it and determine the full impact of the incident, including the estimated number of users impacted. The Service Provider will also be responsible for coordinating the incident communication of ongoing status of incidents with the Service Desk. All communications and updates pertaining to the incident must be captured and documented within the ticket for reporting purposes.

The Service Provider may be required to engage with other Third Parties for the purposes of investigation and resolution. Regardless of what caused the incident no additional fees will be charged to SSC over and above the base resource unit fees defined in the Attachment 3.1 - Pricing Submission Sheet. SSC may request a written report that details the root cause, an analysis, and a procedure and/or plan for correcting incidents. In the event that the incident resolution exceeds the MTRS (Mean Time to Restore Service) service level, the Service Provider will provide options to mitigate the impact or identify temporary workarounds.

2. Enterprise Service Desk Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
General Support			
Provide a single point of contact accessible via telephone, email address, fax, and web-enabled interfaces.	X		
Provide the Service Provider all information necessary to develop training documentation, policy guides, reference manuals, procedures and support scripts necessary for Service Desk staff and technicians to function appropriately.		X	
Provide Service Desk personnel access to ESD's knowledge base to search for information when responding to SSC service requests and incidents.		X	
Develop and maintain training documentation based on existing operational documentation including support scripts.	X		
Maintain Service Desk operations documentation including training documentation and support scripts.	X		
Identify any incidents and service requests and communicate with SSC support teams.	X		This includes any incidents and service requests identified by the Service Provider proactively.
Communicate to SSC support teams, the status of any incidents and service requests, until the incidents and service requests are resolved and closed.	X		Can be done through email notification or via automation. High and Critical can also be performed by the incident Coordination team.
Provide early warning and recommendations to SSC of incidents or problems based on information and knowledge of SSC's operating environment (e.g. common trends, new incidents, call volume spikes, etc.).	X		
Approve action/response to recommendations for incident/problem avoidance recommendations.		X	
Develop a Customer Satisfaction scoring mechanism to measure SSC satisfaction with Service Desk services being provided.		X	Mechanism should have the ability to tie SSC responses to specific Service Desk personnel.

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
Approve satisfaction scoring mechanism developed.		X	
Implement the Customer satisfaction scoring mechanism as approved by SSC.		X	SSC to provide information necessary to support the implementation of the tool (i.e. communications plan).
Schedule operational reviews with SSC (monthly), and highlight opportunities or areas where process improvements could be made to improve service levels, operational performance, or providing other benefits related to Service Desk operations.	X		
Attend operational reviews with Service Provider with SSC (monthly).	X		
Provide a single point of contact who is responsible for interfacing with SSC on matters related to the Service Provider's delivery of Services.	X		SSC will approve this individual.
Identify user training needs based on patterns and frequency of contacts to the Service Desk.	X		
Manage the staff required to provide the Service Desk services.	X		
Maintain Service Desk staffing levels for planned and unplanned contact volume overflows (e.g. emergencies, enterprise application deployments etc.).	X		
Provide projected call volumes and related staffing level requirements.		X	
Take into account the peak volume periods caused by user population imbalances and normal busy periods for users, and provide appropriate staff levels to ensure quality of service is maintained.	X		
Perform minor administrative changes to the phone system in order to meet immediate operational requirements.	X		SSC may, on occasion, perform administrative changes to the phone system with consultation from the Service Provider.
Provide the capacity to increase staffing levels to handle unexpected call volume spikes.	X		

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
Ensure that staffing levels for every shift reflect call volumes patterns	X		
Adjust phone system open and close hours to reflect statutory holidays to ensure non-business hours script scenarios are followed.		X	
Add new Service Desk Agents phones into the system, or change phone assignments with the addition or movement of Service Desk resources.	X		
Keep the inventory of pre-recorded phone system emergency messages current and accurate.	X		
Record emergency broadcast phone system messages live in both official languages when a message is required and when no appropriate pre-recorded message exists.	X		
Record new phone system wait queues and voice mail messages to reflect any changes in procedure		X	
Recommend to the Technical Authority changes to the telephony system script or other functions to enhance performance or meet new procedural requirements.	X		
Coordinate the implementation and testing of all approved changes with Telecommunications and the vendor.		X	
Run the test script following any change to the system during non-business hours to ensure correct functionality is not adversely affected.		X	
Keep the test script current, complete and accurate.		X	
Report all and any incidents affecting the phone system to Telecommunications immediately upon detection.	X		
Work with Telecommunications and the vendor in order to troubleshoot and rectify incidents to restore service as quickly as possible.		X	During regular business hours, SSC will maintain responsibility for the phone system. After hours, the Service Provider may be asked to provide additional support.
Provide a trusted workaround procedure in the case		X	

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
of an incident affecting the phone system.			
Implement trusted workaround procedures until the phone system incident is resolved.	X		
Implement tools necessary to provide Service Desk services and meet SSC informational and functional requirements.		X	
Design, develop, document, and implement manual or backup procedures for Service Desk personnel to follow in the event that the Service Desk tools used to process user contacts fail to operate properly.	X		
Document escalation procedures to be followed in the event that Service Desk personnel are unable to perform any / or part of their job functions because of system, communication, application availability, or other data centre or Service Provider site related problems.	X		
Establish global work processes for all of the Service Provider's Service Desk installations to deliver consistent Services across locations.		X	
Follow global work processes for all of the Service Provider's Service Desk installations to deliver consistent Services across locations.	X		
Execute availability contingency plans for critical systems when and as required.	X		
Develop availability contingency plans.		X	
Ensure availability contingency plans are kept current, complete and accurate and test all and any changes to them.	X		
Report any security breaches immediately such as, but not limited to, reports of viruses to the appropriate authority according to procedure.	X		
Communicate and work with the Security group to remain informed on any security issue.	X		
Control building security access to IT support staff and 3rd party vendors as per established procedures.		X	
Provide strategic planning and final direction with respect to both the current services delivered and any services that will be delivered in the future.		X	

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
Manage and plan the technologies and associated capacity requirements that will be used in the delivery of services.		X	
Manage the service delivery performance for all delivered services.	X		
Manage the progress, to the extent possible, to a standardized IT environment - infrastructure and architecture.		X	
Manage the quality of the services delivered to each customer.	X		
Manage the Client relationships.		X	
Manage the Contracts and Contractor relationships.		X	
Service Desk Support			
Record and classify incidents, including priority of request, received from users and the Service Providers, capturing information and verifying that the Configuration Item (CI) information is correct.	X		
Record and classify incidents received through Level 2 Service Provider's automated monitoring, capturing information and verifying that the Configuration Item ("CI") information is correct.	X		
Interact with different levels of IT technical support groups such as to resolve support issues.	X		
Actively monitor all calls, incidents, service requests, problems and change management tickets for status and ensure the appropriate action is taken according to procedures and prescribed thresholds.	X		
Actively monitor all tickets for critical and high Priority incidents.	X		
Validate the end-user's profile or the Partner Profile to ensure the information is complete and accurate.	X		
Validate that the end-user/Partner is entitled to Service Desk Services. The call may have originated at another Service Desk but re-assigned based on the service support.	X		
Capture/record the details for every contact and assess the end-user's request.	X		
Classify the call according to the available categories and follow the procedures established for the	X		

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
category/call type.			
Work with an Automatic Call Distribution telephony system: log in and out, set status, and generate reports as required.	X		
Review classification of incidents throughout their life cycle to elevate to higher priority level as defined by impact and urgency (or as determined by SSC).	X		
Execute incident management in accordance with approved procedures and policies.	X		
Dispatch/route the call to the appropriate Service Desk, Service Group or 3rd party vendor, if the call cannot be resolved at first point of contact.	X		
Escalate all major incidents.	X		
Identify and communicate problem requests and functionally assign root cause analysis activity to Third Party vendors.	X		
Conduct incident troubleshooting and problem determination for the following areas: network, application, workstation, server, maintenance schedule, I.D. administration (e.g. new logon/account changes), and identification of security incidents.	X		
Check active incident and problem tickets and associate / link required change tickets to them in order to restore service and perform escalations and notifications to affected stakeholders, as per the SoW.	X		
Provide Mainframe IT technical support such as password resets, cancelling jobs, unlocking/recycling user sessions, resetting accounts for Mainframe systems.	X		
Provide Midrange IT technical support such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding application, resetting of FTP accounts, ticket updates based on auto-generated alarms, assisting users with web-based applications for Mid-range systems such as HP/MPE, VAX/VMS, UNIX-based operating systems, Windows NT-based operating systems, and Linux platform.	X		
Establish the criteria for resetting passwords and disclosing them to authorized personnel.		X	

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
Reset passwords upon first contact.	X		
Action voice mail, email messages and self-ticketing tickets and respond to them in a timely manner, within the prescribed SLA time frames.	X		
Perform Quality Assurance review on tickets resolved by resolver groups outside of ESD. The QA score must be determined based on 4 call (live or recorded) and ticket evaluations per agent per month. The Supplier is responsible for conducting these evaluations. The QA evaluation includes 10 questions covering Customer Service etiquette, procedure adherence, and ticket management.	X		
Communication and Notification			
Provide status updates to affected users and Partners.	X		Service Provider to use SSC approved templates and have any custom messages approved by SSC.
Manage user/Partner communications and notifications on multiple user incidents in accordance with customer communication guidelines and style guides.	X		
Act as a communication centre between the user-client community and the support groups for all infrastructure requests, incidents and related activities.	X		
Establish and maintain an efficient two-way communication protocol between all support groups related to any aspect of request satisfaction, incident resolution and change to the infrastructure.	X		
Coordinate and organize the dissemination of relevant information to clients.	X		
Participate in a monthly operations review meeting with SSC where all metrics, reports, corrective action statements and recommendations developed by the Service Provider must be reviewed and discussed for SSC approval.	X		
Incident Management			
Incident detection, recording and reporting.	X		
Incident classification and first-line support (e.g. suggestions to solve or workarounds).	X		SSC has the right to re-classify tickets.

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
Prioritize the incident according to the predetermined incident Classification and incident Priority Matrix.	X		
Incident matching between new incident and known incidents, problems or known errors.	X		
Incident investigation and diagnosis.	X		
Incident resolution and recovery.	X		
Incident closure.	X		
Incident ownership, monitoring, tracking and communication.	X		SSC will provide communications guidelines.
Routing and monitoring of service requests.	X		
Provide technical skills to support applications, maintenance.		X	
Configuration and management of incident management tools.		X	
Problem Management			
Record all relevant details of the potential Problem in the Problem Management Service Management Tool following pre-defined processes and procedures.		X	
Co-ordinate problem investigations, conducting root cause analysis, and identifying recurring incidents and identifying problems opening the associated ticket accordingly per pre-defined procedures.		X	
Actively check all problem records for status and priorities.		X	
Actively check all incident records for status and priorities.	X		
Reference the Known Error Database and Problem Management Tool to ensure that no like records already exist prior to flagging a record as a potential Problem.		X	
Follow all pre-defined process and procedures to ensure compliance to the Problem Management Process.		X	
Coordinate problem investigations, conduct root cause analysis, and identify recurring incidents and identify problems opening the associated ticket accordingly per pre-defined Problem Management		X	

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
procedures.			
Implement pre-defined Problem Management procedures.		X	
Perform quality assurance by reviewing ticket resolution information to ensure that the event is indeed resolved permanently.		X	
Reference the Known Error Database in order to restore service.	X		
Create a new Known Error Record if required in pending status for Problem Management's approval.	X		
Account Administration			
Provide account administration.	X		
Manage user IDs, create IDs, passwords and customer access as required and authorized.	X		
Co-ordinate and track user ID creation, ID changes and password resets for SSC managed applications.	X		This involves accepting requests for SSC application ID requests, forwarding to the appropriate application support team and tracking the request to ensure that it is completed as per Service Desk processes.
Create and/or modify account administration documents, processes and guidelines, modification of processes and guidelines.		X	
Perform checks of the necessary IT environment, such as ensuring client service is uninterrupted and monitoring of job queues and server loads.	X		
Check server space utilization according to established guidelines.	X		
Perform Service Desk account security such as obtain accounts, establish accounts, implement accounts, and enforce accounts as necessary.	X		
Update end user Partner profiles and access groups.	X		
Disable/delete accounts following the approved disabling procedures, including purging deactivated	X		

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
accounts and associated data on a monthly basis.			
Obtain/establish, implement and enforce security procedures that will ensure the safety of the corporate and individual's information for all accounts processed by the SD.	X		
Manage, prevent, resolve and report account administration integrity issues.	X		
Monitor server space utilization according to technical support groups' guidelines.	X		
Assist end users in the addition, creation and changes of logon IDs according to SSC defined processes for access requests.	X		
Create new logon IDs, file shares and appropriate directories.	X		
Set up end users with standard site logon configuration files.	X		
Perform end user ID deletes including removing IDs and delete, file share and permission management, archive or move associated data to a new owner.	X		
Make logon ID changes in user privileges as requested via SSC defined access request process.	X		
Request Fulfilment (RFL) and Change (RFC)			
Validate the request and ensure the proper information and approvals have been obtained from the appropriate approval authority.	X		
Perform checking of the necessary IT environment for change management such as requests for change and account administration aspects to ensure client service is uninterrupted.	X		
Initiate change management tasks such as validation of requests, determine and tailor requests, task, workflow, quality assure, close requests, report.	X		
Record all details of the request per pre-defined templates.	X		
Classify the RFC and determine the change model.	X		
Assign the RFC to the appropriate service groups.	X		
Monitor the RFCs requesting status updates and updating the request.	X		

Enterprise Service Desk Activities	Service Provider	SSC	SSC Comments
Perform required notification and escalation per the pre-defined process and procedures.	X		
Modify task and workflows.	X		The Service Provider must conform to workflows and tasks that are developed by and spanned across multiple departments and partners where applicable.
Inform appropriate support groups of issues related to a change request or service requests, and escalate any issues to the relevant group(s).	X		
Ensure work performed is accounted for and required actions are taken with respect to the request.	X		

d. Transition Services

The transitions in (from the current Service Provider) and out (to any future Service Provider) must be accomplished in a manner that is non-disruptive and well planned to accommodate the progressive takeover of the service delivery. The transition processes must minimize risk to the quality of service, and cause minimal impact to clients' operations.

1. Transition-In Plan

Within 14 calendar days of the Contract Award Date, the date of issuance of the Contract by SSC, the Service Provider must provide to SSC a Transition-In Plan ("TIP") for approval and acceptance. It must be sufficiently detailed to clearly identify how the Service Provider will transition-in all of the Enterprise Service Desk and Enterprise Command Centre services from the current Service Provider. At a minimum, the TIP must include, but is not limited to:

- How the Service Provider will obtain an understanding of the entire Enterprise Service Desk and all Functions and Sub-Functions contained within
- How the Service Provider will staff, train and prepare their workforce so that they are fully capable of providing Services (i.e. Resource Plan)
- Identification of the Key Resource names and security classifications so site security accesses can be pre-arranged and the beginning of the submission of the résumés for the remaining Key Resources who will make up the total Key Resources to be working at the start of Transition-In activities
- ESD knowledge transfer strategy for all Key Resources and for all Service Provider resources;
- Service Provider's proposed transition schedule
- Training plans and methodology (which would include but not be limited to: shadowing with outgoing contractors, site visits, familiarization with tools, study of SSC-provided operational documentation and internal assessment methodology)
- How the Service Provider will obtain an understanding of the ESD and technical environments, support structure and business relationships; and
- Reporting strategy including:
    - Weekly Transition-In Reports (including but not limited to attainment levels per training category and resource levels);

- Weekly Operational Reports, as described in Appendix A to Annex A
- Establishing service level reporting, as described in Appendix A to Annex A
- Establishing quality reporting, as described in Appendix A to Annex A
- Transition-in incident reporting; reporting (including but not limited to Daily Backlog Report and Activity Plan as described in Appendix A to Annex A
- Service Provider-related escalation process/governance

The 30 calendar days immediately following the date of acceptance of the TIP is the Transition-In Period, during which the TIP must be implemented by the Service Provider. SSC will not change the technical infrastructures or environments identified in the RFP during the Transition-In Period. The Transition exercise is of critical importance to ensure that the Service Provider is fully capable of performing the responsibilities of the Function at Contract Start Date and to demonstrate to SSC that the expected levels of service are being achieved.

On the day after the date of acceptance of the TIP, the Service Provider must provide, on site, the Resources outlined in task authorization in accordance with Appendix C to Annex A – Tasking procedures, in the event that the resource proposed in the Service Provider's Proposal is unavailable through no fault of the Service Provider, a substitute approved and accepted by SSC. This substitute must meet all of the requirements associated with the category as per Appendix D to Annex A – Resource Assessment and Criteria response tables, meet the language requirement relative to the ratios identified in Section 2.4, and hold a valid security clearance at the requisite level to be accepted.

SSC will ensure that the service documentation maintained by the incumbent Service Provider will be complete, approved by SSC, and available for use by the new Service Provider upon contract award.

The Transition-In must be completed by the Service Provider within 30 calendar days following the date of acceptance of the Transition-In Plan [the "transition" – in TIP]. The Contract Start Date is the day immediately following completion of the 30-day Transition-In. At the Contract Start Date the following must have occurred:

a) The Functions must be transitioned to new Service Provider
b) The Key Resources must be autonomous in their new roles
c) The Service Provider must have provided the minimum staffing requirement of Key Resources as identified, or their equivalent as approved by SSC
d) The Service Provider must have taken full responsibility for the delivery of all Functions.

SSC will pay the Service Provider as per the Request for Proposal if all of (a) through (d) above have occurred.

1. Transition-In Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Transition-In Activities	Service Provider	SSC	SSC Comments
SSC will not change the technical infrastructures or environments during the 30-day Transition-In Period.		X	
Ensure key resources are available on a full time basis from the first day of the Transition-In Period, and for a minimum of 6 months following the end of	X		

Transition-In Activities	Service Provider	SSC	SSC Comments
the Transition-In Period.			
Ensure key resources are available to perform certain work outside of regular business hours as required.	X		
Key Resources must be made available as required by SSC, and will be expected to learn the key aspects of the Service Desk Functions from the incumbent resources during the Transition Period.	X		
Key Resources must transfer this knowledge to the winning bidder's remaining contractor resources by the Contract Start Date.	X		
The resources proposed by the winning Bidder must have the experience, skills and knowledge to perform their roles, and may require specific knowledge transfer on specific aspects of the SSC domain or systems to assume operational responsibilities.	X		
Contractor must ensure that Resource availability is maintained and that the Contractor's Transition activities do not cause service disruptions.	X		
If an equivalent resource is provided, the resource is subject to approval by SSC.	X		
Contractor must provide a weekly "Transition-In" report detailing the status of all "Transition-In" activities as well as transition issues, mitigation, progress, recommendations and any other pertinent details.	X		
All requirements of the Transition-In Plan must be implemented on schedule.	X		
Contractor must carry out the transition of its staff and processes associated with a Function such that it is ready and able to carry out all work associated with the Function by the end of the Transition-In Period.	X		
The Transition exercise is of critical importance, to ensure that the Contractor is fully capable of performing the responsibilities of the Function and to demonstrate to SSC that the expected levels of service are being achieved.	X		
SSC shall notify the Contractor, in writing, of acceptance of the Transition when the Contractor has demonstrated to the satisfaction of SSC that it is ready to carry out all of the work described in this		X	

Transition-In Activities	Service Provider	SSC	SSC Comments
SOW.			
All costs associated with the Transition shall be the responsibility of the Contractor.	X		

2. Transition-Out Plan

At the end of the Contract Period, the Service Provider must assist with the transition of the Domain to a new Service Provider. The Service Provider must cooperate with a new Service Provider to ensure that smooth and seamless transition of services occurs. The Service Provider must ensure that overall operational availability is not disrupted; existing service levels are maintained and Contract deliverables continue to be delivered while transition and knowledge transfer to a new Service Provider or to SSC staff occurs.

1. Transition-Out Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Transition-Out Activities	Service Provider	SSC	SSC Comments
Transition-Out			
Ensure that all documentation (i.e. operational, training, reporting, etc.) is up to date and accurate. Copies of all documentation must be provided within 2 working days on written request from SSC.	X		
Ensure operational procedures are up to date and accurate.	X		
Ensure operational checklists are maintained to current requirements and are complete and accurate. Copies of these checklists must be provided within 2 business days on written request from SSC.	X		
Continue to meet established operational service levels and targets.	X		
Continue to meet existing service level targets as they relate to incident management and change management.	X		
Allocate the necessary time to assist in one-on-one knowledge transfer to the incoming Contractor.	X		
Prepare and deliver detailed transition documentation for presentation to SSC to be utilized with the incoming Contractor. The transition documentation and presentations must be provided for each Function and Sub-Function within the Request for Proposal. The documentation must describe, in the necessary detail, all the pertinent and	X		

Transition-Out Activities	Service Provider	SSC	SSC Comments
important details necessary for a successful transition to the incoming Contractor.			
Prepare weekly Transition-Out reports.	X		

5. Resource Requirements.

This section details the resource requirements required to perform the ESD functions.

b. Expected Quality

The expected approximate annual volumes or the Enterprise Service Desk are as follows:

- Calls – 58,500
- Emails – 238,000
- Service Requests – 266,000
- Incidents – 18,500
- Service Requests, Incidents, and Change Requests from other tools – 26,500

c. Resource Positions

Service	Function	Position Title	Qty
ESD	Domain Management	Domain Management SDM	1
ESD	Domain Management	Domain Team Lead	1
ESD	Domain Management	Domain Reporting Analyst	1
ESD	Domain Management	Domain Quality Analyst	1
ESD	Domain Management	Domain Client Delivery Executive	0.5
ESD	Incident Management	Incident Management Senior SDA	5
ESD	Incident Management	Incident Management Team Lead	4
ESD	Incident Management	Incident Management Escalation Coordinator	4
ESD	Call Management	Intermediate SDA	37
ESD	Call Management	Junior SDA	34

Position Descriptions

The Domain Management Service Delivery Manager (“SDM”) manages the daily operations of the operations and coordination staff. They are the single point of contact for day to day service delivery, and ensure performance and quality of service is met.

Domain Management SDM must meet the following requirements

- 7 years of experience in the management of IM/IT service desks, teams, budgets and contracts in a Government or large corporate environment of 5,000 or more end users

- 7 years of experience producing and implementing comprehensive Monthly Action Plans (MAP) for Service Desk optimization such as:
  - SD metrics
  - implementation of SD process improvements
  - training gaps
  - client service expectations
- 7 years' experience defining technical specification workload estimates in relation to SD services
- 7 years' experience ensuring that the Service Level Targets are met and that those missed are documented
- 7 years' experience in monitoring and testing contingency plans for critical Service Desk systems
- 7 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products such as MS Office. Technical support can include such as password resets, hardware issues, software related issues such as non-responding applications, identification of security incidents such as viruses and malware security incidents such as viruses and malware as well as any other type of issues related to Infrastructure component.
- 7 years providing expertise and guidance with regards to a Service Desk environment for Service Desk functions related to workstations, server and client environments
- 7 years' experience implementing corrective actions in a call centre environment related to call, incident, Problem and change management and escalation processes
- 7 years' experience reviewing service management status reports including data related to quality assurance, daily and weekly call statistics, issue/problem resolutions
- 7 years' experience in the analysis of IT Service Desk workload reporting to determine process improvements in areas such as call resolution, customer service
- Valid Federal Government Level II Secret Security Level Clearance

Domain Team Lead

The Domain Team Lead is a Supervisor, managing employees and overseeing operation of the Service Desk.

Domain Team Lead must meet the following requirements

- 5 years' experience providing Information Technology technical support services in client operating systems, networks operating software l or commercial-off the-shelf ("COTS") office products (MS Office). Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware as well as any other type of issues related to Infrastructure component.
- 5 years' experience in the management of IT projects and teams
- 5 years' experience implementing Management Action Plans (MAP) in a Service Desk environment such as:
  - SD metrics
  - implementation of SD process improvements -training gaps
  - client service expectations

- 5 years providing expertise and guidance with regards to a Service Desk environment for Service Desk functions related to workstations, server and client environments
- 5 years' experience implementing corrective actions in a call centre environment related to call, incident, problem and change management and escalation processes
- 5 years' experience determining technical workload specifications in relation to the Service Desk environment
- 5 years' experience reviewing service management status reports including data such as quality assurance, daily and weekly call statistics, issue/problem resolutions
- 5 years' experience in the analysis of IT Service Desk workload reporting to determine process improvements in areas such as call resolution, customer service
- 5 years' experience in the provision of IT support client services within an IT environment for a Government or large corporate environment of 5,000 or more end users
- Valid Federal Government Level II Secret Security Level Clearance

Domain Reporting Analyst

The Domain Reporting Analyst gathers and performs analysis on statistical data. They then use this to generate reports on Service Desk performance.

Domain Reporting Analyst must meet the following requirements

- 4 years' experience producing reports for a Service Desk environment such as overall expertise, knowledge and performance levels for each specific area of expertise, such as Service Desk Agents (SDA) for Call, incident, Problem, Change, as well as Account Administrator (AA), Tasks Flow Controller (TFC) and Change Requests
- 4 years' experience in the use of spreadsheets for tracking workload metrics on calls, incidents, problems and changes on a daily, weekly, monthly and quarterly basis
- 4 years' experience in tracking of metrics related to a Service Desk environment such as metrics and volumetric that demonstrate optimal performance of Problem resolution and request processing
- 4 years' experience producing documentation related to collection of metrics such as weekly activity statistics, call metrics, service management metrics, monthly resource requirements based on workload, SLA obligations
- Valid Federal Government Level II Secret Security Level Clearance

Domain Quality Analyst

The Domain Quality Analyst is responsible for reviewing the quality of a percentage of tickets, and providing feedback to the agent.

Domain Quality Analyst must meet the following requirements

- 4 years' experience in providing quality assurance in a Service Desk environment in preparing things like quarterly reports on findings, deficiencies, degradation, problems with existing processes, procedures, Service Desk Agents and recommended corrective measures and/or improvements

- 4 years' experience with an enterprise class IT Service Management record, prioritize, match against other tickets in the system , track, document, assign and close call/incident, problem and IMAC/change tickets
- 4 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required
- 4 years' experience in the analysis of quality assurance data related to a Service Desk environment such as the effectiveness and performance of all service desk tasks
- 4 years' experience in the use of spreadsheets for quarterly samples tickets (calls taken and problem number assigned) and reports detailing Service Desk Agent resolution rates of problems
- 4 years' experience in tracking of quarterly samples tickets (calls taken and problem number assigned) and reports on the Service Desk's quality of Service Requests
- 4 years' experience producing reports for a Service Desk environment such as on the integrity and day-to-day procedures of the SD indicating where the quality of work has degraded, maintained, or improved
- 4 years' experience producing documentation related to collection of metrics such as problem resolutions and request processing
- Valid Federal Government Level II Secret Security Level Clearance

Domain Client Delivery Executive

The Domain Client Delivery Executive oversees the delivery of the contract.

Domain Client Delivery Executive must meet the following requirements

- 10 years' experience in developing and monitoring of Service Desk action plans, policies, and guidelines
- 10 years' experience in the analysis and engineering of Information Technology processes to optimize operations
- 10 years' experience in analysis of Service Desk reports to ensure client service objectives are met such as overall satisfaction and service levels are being met and to address Service Desk delivery issues
- 10 years' experience in customer relationship management with government departments or large private sector organizations with over 5,000 resources
- 7 Project Management experiences and valid certification
- Valid Federal Government Level II Secret Security Level Clearance

Incident Management Senior Service Des Agent

The Incident Management Senior Service Desk Agent ("SDA") is an experienced resource acting as a point of contact for internal escalation related to issues that Service Desk Agents are unable to resolve. They are also specialized in processes and procedures in a specific stream.

Senior Service desk Agent must meet the following requirements

- 4 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close Service Request l/incident, problem and IMAC/change tickets
- 4 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as

non-responding applications, identification of security incidents such as viruses and malware as well as any other type of issues related to Infrastructure component.
- 4 years' experience working with an Automatic Call Distribution telephony system log in and out, set status, generate reports as required
- 4 years' experience providing coaching/mentoring to team members in an IT environment
- Valid Federal Government Level II Secret, or Enhanced Security Level Clearance

Incident Management Team Lead

The Incident Management Team Lead provides direction, instructions, coaching and guidance to a group of individuals.

Team Lead must meet the following requirements

- 5 years' experience working with an enterprise class IT Service Management tool, record, prioritize, match against other tickets in the system , track, document, assign and close Service Request l/incident, problem and IMAC/change tickets
- 5 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products. Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware of security incidents such as viruses and malware as well as any other type of issues related to Infrastructure component.
- 5 years' experience interacting with different levels of IT technical support groups such as to resolve support issues, participate in projects
- 5 years leading a team of professionals in the delivery of IT services such as:
  - call management
  - on-line support
  - problem and incident management
  - escalation
- 5 years' experience in the documentation of technical IT solutions
- 5 years' experience providing coaching to IT clients and team members
- Valid Federal Government Level II Secret Security Level Clearance

Incident Management Escalation Coordinator

The Incident Management Escalation Coordinator monitors incidents and changes, performing notifications and escalations to the appropriate contacts as necessary.

Escalation Coordinator must meet the following requirements

- 3 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close Service Request l/incident, problem and change tickets
- 3 years' experience in analysis and triage of IT service desk incidents
- 3 years' experience interacting with different levels of IT technical support groups to check active incident, problem and change tickets against service level targets and perform escalations and notifications to affected stakeholders
- Valid Federal Government Level II Secret Security Level Clearance

Intermediate Service desk Agent

Intermediate Service Desk Agent ("SDA") answers calls, performs basic troubleshooting and attempts first call resolution.

Intermediate Service Desk Agent must meet the following requirements

- 3 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf (COTS) office products. Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware
- 3 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close service request l/incident, problem and change tickets
- 3 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required
- Valid Federal Government Level II Secret, or Enhanced Security Level Clearance

Junior Service Desk Agent

Junior Service Desk Agent ("SDA") is responsible for answering simple Level 1 calls and attempting first-call resolution. Examples of this type of call would be a password reset or an account unlock.

Junior SDA must meet the following requirements

- 2 year experience OR an acceptable combination of education, training, and/or experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products Technical support can include password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware
- 2 year experience OR an acceptable combination of education, training, and/or experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close service Request l/incident, problem and/change tickets
- 2 year experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required
- Valid Federal Government Level II Secret, or Enhanced Security Level Clearance

PART 3
SSC ENTERPRICE COMMAND CENTRE AND DATA CENTRE OPERATIONS

Table of Contents

1. Introduction

The scopes of the Services that are the subject of this RFP are detailed in Section 4 of this document, and include the following:

- Service Management Functions (see Section 4.1 for more details);
- Enterprise Command Centre ("ECC") (see Section 4.2 for more details);
- Transition Services (see Section 4.3 for more details).

Shared Services Canada ("SSC") has written the service descriptions to focus on specific outcomes and activities the Services Provider must execute.

2. Contract Terms

2.1 Location

All services will or can be delivered from the following locations; however, the majority of the resources will be located in the National Capital Region:

- KEDC - 350 King Edward Ave., Ottawa, ON
- APDC - 700 Montreal Rd., Ottawa, ON
- MCDC - 1600 Tom Roberts Rd., Ottawa, ON
- PDLC - 550 Place de la Cite, Gatineau, QC
- GPC – 625 Blvd du carrefour, Gatineau, QC
- 2300 St. Laurent Blvd., Ottawa, ON
- 875 Heron Rd., Ottawa, ON (backup site)
- 1200 Vanier Parkway, Ottawa ON
- 1081 Main St., Moncton, NB
- 715 Peel St., Montreal, QC
- 494 Dundas St. East, Belleville, ON
- 2121 TransCanada Highway, Dorval, QC
- 37 Centurion Close., Borden, ON
- 11 Laurier Avenue , Gatineau, QC

In the event of a disaster at one of the present locations the key operations of the ECC resources shall be reassigned to a Disaster Recovery ("DR") site within the National Capital Region (NCR) to resume operations until the situation is rectified, as per current SSC Business Continuity procedures. SSC will provide the Service Provider with sufficient notice of any facility (or service delivery location) changes. Changes to the location will not trigger a change to pricing or other expenses. Bidders are expected to take this into consideration in their pricing responses.

2.2 Workstations and Telephones

During the Contract period, SSC will provide workstations for the Service Provider's resources to use. The Service Provider will also be provided with an office phone system. Bidders are encouraged to review the Financial Responsibility Matrix tab in the Pricing Template Attachment 3.1 for clarity on what SSC will provide and what the Service Provider is responsible for providing in their pricing submission.
The Service Provider will be responsible for providing its resources with smart phones as required at their own expense.

2.3 Operating Hours

ECC event management services must be provided on a 24 hours a day, 7 days a week, and 365 days a year including all holidays. There are some activities that are not required to be delivered on a 24 x7 basis and those can be delivered during the Government of Canada core business hours which are (07:00 to 17:00) Monday to Friday excluding federal statutory holidays.

2.4 Language Requirements

There is no bilingual requirement for the Enterprise Command Centre resources.

2.5 Security Clearance Requirements

All Enterprise Command Centre resources must obtain Level II Secret Government of Canada security clearance, and maintain Level II Secret security clearance for the duration of their employment. The ECC requires 100% Secret security clearance for its resources.

3 Current State Summary

Since 2013, SSC has outsourced their ECC and Direct Operations functions to a Services Provider ("SP"). The contract with the SP is set to expire on June 2018.

The purpose of this description is to provide Proponents with context and is not intended to be an indication of how SSC would like to have their services delivered.

The SP was selected through competitive tender and operates under a contracting framework that provides SSC with the required qualified resources. The Service Provider is providing resources, with some Government of Canada employees providing overall guidance and service management functionality.

All SSC and Government of Canada data currently resides in Canada and this requirement must be maintained throughout the duration of the subsequent contract.

3.1 Enterprise Command Centre (ECC) Overview

The ECC scope encompasses a wide variety of platforms, and applications in order to manage the complex environment of SSC.
ECC provides support for: Event Management Mainframe, Event Management Midrange, and network monitoring and support. The additional duties include tape and facilities management. For this contract, ECC activities takes place in three major data centres, with onsite teams 24 hours a day, seven days a week, including holidays. The Aviation Parkway Data Centre ("APDC"), the King Edward Data Centre ("KEDC"), and the MacDonald Cartier Data Centre ("MCDC"), which is located in the National Capital Region ("NCR").

A fourth data centre, the Summerside Data Centre ("SSDC") houses a mainframe. The mainframe in this data centre is supported remotely from the King Edward Data Centre on a 24x7 basis. A fifth data centre, the St. Laurent Data Centre ("SLDC") this data centre is supported remotely by Event Management Mainframe from the King Edward Data Centre on a 24x7 basis. A sixth and seventh data centre exists at Library & Archives Canada ("LAC"); one located at Place de la Cite (PDLC) and the other located at Gatineau Preservation Center (GPC) in Gatineau, Quebec and is supported 8x5 by a dedicated team of 2 operators. Of the 2 day time operators, one resource must have a tape background. These locations are subject to change but will remain located within the National Capital Region.

The primary responsibilities of Event Management Mainframe are system monitoring, batch processing, and incident and change coordination. Activities in this environment include providing level 1 support for 47 production, engineering, and disaster recovery MVS and VMLinux images, distributed between the King Edward Data Centre ("KEDC"), the MacDonald Cartier Data Centre ("MCDC"), the Summerside Data Centre ("SSDC") and the St. Laurent Data Centre ("SLDC"). Among the clients supported are those internal to SSC and partners. Incident escalation and resolution for batch jobs is handled here. Additionally, ECC monitors and coordinates changes during weekend maintenance windows. The 47 LPARS monitored by ECC are comprised of various production, test, development engineering, and disaster recovery images. Each type of image requires a different level of monitoring from ECC and varies from critical to as-required.

Event Management Midrange provides various levels of support for over 3800 physical and virtual servers mostly within the NCR. Depending on client service level agreements (SLAs), the level of responsibility varies from IR monitoring and resolution, backup monitoring and resubmission to facilities management, and courtesy reboots. Operating Systems supported include various Windows and UNIX platforms. The majority of the servers and equipment in the scope of the Midrange Operations function are located at the APDC, KEDC, MCDC and LAC data centres, along with a number of Public Key Infrastructure ("PKI") servers located at KEDC. Event Management Midrange also performs digitization archival and restoral functions for LAC clients.

Tape Management provides tape and storage expertise in addition to the event management. The tape function is required at APDC, KEDC, MCDC, and LAC data centres, providing tape library, inventory, handling and tape monitoring. These tasks require physical handling of tape and equipment along with shipping and receiving, so that tapes can be stored off site. These resources will monitor all tape jobs, errors, re-initiate jobs and provide support as an extension to the second level tape and storage teams, as they will be located on site.

Facilities Management provides facilities expertise in addition to the event management. The facilities function is required at APDC, KEDC and MCDC data centres. At these sites the resources are required to do physical walk around to inspect servers, data centre hardware, and environmental equipment for any abnormalities. These tasks also include the requirement to install and remove equipment, as required to minimize the need for support and third party vendors to come on site. Part of the responsibilities is to provide escorting to support and vendor personnel and track all security access.

3.1.1 Enterprise Command Centre Tools

Tool Name	Tool Description	Tool Function / Purpose	ECC - KEDC	ECC - APDC	ECC - MCDC
ECD	Service Management : Ticket-System	(a)To track incidents for Command Centre Workload (d) Used to validate Datacentre access (e) Used to validate datacentre access (h) incident coordination and tracking		YES	YES
Info/Man	Service Management : Legacy Ticket-System	(a) Service Management Tool (Mainframe workload) (b, d and e) Logging of incident records, change requests, service requests and work orders.	YES	YES	YES
HMC (Hardware Management Console)	Monitor	(a) Mainframe Hardware (b) HMC is used to interact with the CPU (IPL, Reset clear, activate etc.) (f) Mainframe Hardware management console	YES		

OPS/MVS		A monitor controls all LPAR images. A full automation suite is supported, and its activities include message suppression, error notification, automated start-up/shutdown of online environments, and automated escalation via pager. Manually intervention is also used to start / stop / recycle a component	YES		
Automation Point	Mainframe Console	Access to all the CPU's LPAR's master consoles & alternate consoles, console operator interacts via MVS and JES2 commands, operator replies etc.	YES		
TWS (Tivoli Workload Scheduler)	Batch processing tool	(a) Monitor Production Schedule during off-hours (b) CIPO - Tivoli Workload Scheduler used to monitor, edit JCL, restart, cancel, mark jobs or applications complete. (i) Batch monitoring and control	YES		
CA7 & CA-7 GUI	Batch processing tool	Most SSC Internal applications - Monitor, Edit JCL, Restart, cancel, force jobs or schedules, remove or add requirements. Sends E-mail notifications	YES		
TSM (Tivoli Storage Manager) MAINFRAME MID-RANGE	(a) Tape System Backup (b) Used to manage SAN media environment	(a) SAN Media Mgmt Tool (i) File and Volume management (b and e) Used to manage MID-RANGE SAN media environment	YES	YES	YES
Control-T	Tape Management system Mainframe	Report Schedule and Tape Management	YES		
SDSF (Spool Display and Search Facility)	(a) Spool Display and search facility for MF (b) For MF to view online output	For MF to view online output	YES		
iEService Provider portal (Tivoli)	ECC Dashboard	(b) Dashboard to Monitor, assign, take ownership, process events, access Infoman / web PKI Alerts (e) dashboard for monitoring/actioning Alerts	YES	YES	YES

Online datasets containing Batch Production schedules, located in various members created by clients.		Print / monitor / verify / rerun / suspend or escalate/ backup & restore	YES		
MVS (Multiple Virtual Storage)	Operating system	MVS Commands used to manipulate MVS (display devices, Chpid, outstanding replies, active jobs, send user a message etc.)	YES		
JES2 (Job Entry Subsystem)	Sub system (for O/S)	Jes2 commands used to manipulate the subsystem (hold, cancel, release job, etc. used to manipulate the printer	YES		
ISMF (Interactive Storage Management Facility)	Sub-system (for O/S)	Used to display, locate, eject media etc.	YES		
VMCF (VPS Monitor & Control Facility)	Mainframe Console	VPS Monitor and control system used to display, start stop recycle printers	YES		
Stateman		Used in conjunction with OPS/MVS, rule based system which creates OPS/MVS incidents where console staffs need to intervene to get system back on track.	YES		
NM (Notification Manager)		Notification manager has several methods to notify operations of an alert. By sending alert message to one of the pagers, if unsuccessful sends the notification to a Pop-up Wizard on the desk top, and if all else fails sends an e-mail to the operations group.	YES		
3270 Emulator	Virtual machine software	Used to access and manage the CPU's Lpars (MVS images)	YES	YES	TES
PCOMM		Alternate method to access the CPU's Lpars (MVS Images)	YES		

IService ProviderF Primary Option Menu all Lpars	Sub-system for O/S	There are too many options within this menu to mention, some of the basics are (SDSF, IOF, OPS/MVS calendars, Scheduling & SSM Resources, Perform utility functions ALL, access library DB's, TSO command prompts etc.)	YES		
Virtualization Engine TS7700(Hydra)		Management Interface used to monitor VTS components (Tape Virtualization) 256 virtual tapes drives available at KEDC & MCDC for processing workload. VTS has the ability to failover to an Alternate Site if required.	YES		
Putty	Network Management	(a) Configure and Manage Routers/Switches (d and e) Used to connect to UNIX MID-RANGE servers		YES	YES
VMWare		Used to access alternate network	YES		
VMWare V-Sphere		Used to connect to MID-RANGE VM servers	YES	YES	YES
Cisco Any connect		Used to connect via Entrust for on-call support with system level access (remotely) (d and e) Used to connect to various network segments (MID_RANGE)	YES		YES
Entrust		(b, d and e) Used for Public Key Infrastructure (PKI) to encrypt & decrypt	YES	YES	YES
SiteScan	Datacentre Facilities Monitor	(b) Monitors Environmental in PDP Server Room (f) Environmental monitoring: power A/C etc.	YES		
Cappello	Datacentre Facilities Monitor	(b)Monitors Vancouver Data Centre Environmentals (e) Monitors MCDC and Vancouver Datacentre Environmentals	YES		YES

ISX Struxure Ware Central	Datacentre Facilities Monitor	Monitors Quebec City Datacentre Environmentals (d and e) Used to monitor HVAC environmentals	YES	YES	YES
VNC Viewer	Datacentre Facilities Monitor	Used to monitor the PDP Datacentre environmentals from APDC		YES	YES
VCI	Datacentre Facilities Monitor: MCDC	Used to monitor the MCDC Datacentre environmentals			YES
ForeSeer	Datacentre Facilities Monitor	(a, d and e) Monitors infrastructure (UPS, Generators, Temperature etc)		YES	YES
Watchdog	Automated HIGH severity notification system	Monitors and Notifies on: Severity 1 and 2 incidents	YES		
E-mail		E-mail is used for general purposes, but also as a form of alerts notification from CA7 (late jobs, or schedules, jobs stuck in RDY or Skeleton status) , PKI server errors(Lacerta), or PENMOD monthly batch started, batch failed out and or ended successfully) ETC.	YES		
VMWare Workstation		(b) Used for Server access when connected to different network segments. (d and e) Used for MID-RANGE server access when connecting from different network segments	YES	YES	YES
JADE		Used to monitor PKI CRL's	YES		
Nagios	'Event' Monitoring Tool	(i) Monitoring of Servers, Network, Operational jobs, etc. (d and e) Used to monitor MID-RANGE Alerts		YES	YES
OPEN NMS	'Event' Monitoring Tool	Used to monitor Server alerts		YES	YES
Net IQ	'Event' Monitoring Tool	Used to monitor Server alerts		YES	YES
WinSCP	Used to connect to Unix Servers			YES	YES

CommVault	Backup software Vault Tracker Feature	Used to manage and monitor backup services at LAC			
V-Gadget	Used to monitor network drive utilization			YES	YES

4 Service Descriptions

This section details the service requirements the Proponents will be expected to include in their Proposal and pricing. These services do not necessarily reflect what or how services are currently delivered by the Current Service Providers.

4.1 Service Management Functions

Service Management Functions Services are activities that the Service Provider must perform across all functional areas.

Where there is an impact or interaction with SSC, the Service Provider is expected to deliver the Services using industry standard methodologies and market best practices. SSC may request documentation that provides proof of this. The Service Provider will be expected to follow relevant SSC policies and procedures.

4.1.1 Governance

The objective of Governance is to:

- Monitor and ensure consistent quality for services being delivered to SSC by the Service Provider;
- proactively identify, assess and mitigate risks (both operational and reputational) to SSC stakeholders and ensure compliance to SSC policy and procedures;
- ensure interpretation and compliance to the contract and changes to the terms of the contract and/or SLAs;
- monitor and ensure consistent strategic alignment between stakeholder strategies and service requirements to the Service Provider performance;
- develop, implement, and manage processes such as incident, event, problem, change, and configuration management;
- ensure appropriate levels of engagement between internal stakeholders and the Service Provider at the right point in time in the governance processes;
- provide central reporting and proactively identify areas of improvement;
- provide a continuous improvement framework which strengthens operational performance and fosters the development and implementation of technologies that are in line with technology standards and industry best practice;

4.1.1.1 Governance Responsibility Matrix

Where indicated below with an “X”, the Service Provider must provide the services.

Governance Activities	Service Provider	SSC	SSC Comments
ECC Management			
Implement approved management processes.	X		

Governance Activities	Service Provider	SSC	SSC Comments
Establish mechanisms for ongoing working interfaces (e.g. daily, weekly or monthly meetings and quarterly reviews) with team members managed under the ECC contract as well as personnel associated with other contracts.	X		
Participate in and lead projects as required.	X		
Establish the necessary management structure and related processes to ensure that all responsibilities that are specified in this SOW are carried out such that the terms and conditions are met.	X		
Liaise with various work units and personnel to determine resource requirements as necessary to complete project work.	X		
Implement processes in consultation with various work units and personnel which will track all new work and project related activities concerning ECC activities.	X		
Plan, manage and execute all Contracted activities.	X		
Identify, define and report on workload metrics that best measure the performance of all personnel and the overall operation.	X		
Oversee workload metric data and reports.	X		
Implement incident/problem/event management and escalation processes as set out in appropriate guidelines.	X		
Liaise with various work units and personnel to address issues affecting day-to-day operations.	X		
Work with various work units and personnel to define appropriate paths for the flow of Contract information and status.	X		
Provide 24 hours per day, 7 days a week, 365 days per year a Duty Manager role for management escalation/resolution of all high and critical severity ECC related problems.	X		
Develop, write, maintain and follow all processes, procedures and checklists for the successful delivery of this function.	X		

4.1.2 Reporting

The Service Provider must develop, deliver and maintain a system and processes for specific Workload Metrics (WM) to: collect, store, query and report information that identifies and measures the volume, quality and service level of work performed and the resources required to perform work associated. This Workload Metrics System (WMS), including associated reports, must provide SSC with the necessary information to fully monitor operations.

Within the first 3 months following the Contract Start Date, the Service Provider must provide to SSC, its proposed WMS, including sample reports that will use specific Workload Metrics. SSC retains the right to request further development, changes and further reports from the Service Provider to be included in the WMS. SSC's approval of the WMS will be provided through written communication. The WMS and reports must be prepared and submitted to SSC every calendar month, as described below, or within 5 business days upon written notice by SSC.

At any time, SSC is entitled to access and audit any Workload Metric and Performance Measurement reports and systems for completeness, accuracy and content. A complete list of reports is defined in Appendix A to Annex A

4.1.2.1 Reporting Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Reporting Activities	Service Provider	SSC	SSC Comments
Design, develop, maintain and deliver reports on SLA and KPI's requested by SSC.	X		
Provide reporting analysts to address periodic ad hoc reporting requests regarding user contacts and SSC information, to be approved by authorized SSC personnel.	X		
Provide access to raw data captured within the service management tool for consumption and manipulation by customer analysts and management.	X		
Track workload metrics on calls, incidents, events, problems and changes on a daily, weekly, monthly and quarterly basis.	X		
Explain and demonstrate monthly the human resource usage based on workload and metrics. Report monthly on the resource requirement for each process based on workload. Demonstrate and report that quality thresholds for each indicator for each process are met.	X		
Report monthly on overall expertise, knowledge and performance levels for each specific areas of expertise such as junior, intermediate and senior personnel	X		
Report on general performance relative to SLAs' obligations and objectives, (i.e. met or not met, or the	X		

Reporting Activities	Service Provider	SSC	SSC Comments
proportion of time taken).			
Report quarterly on the integrity and day-to-day procedures reviewed, indicating where the quality of work has degraded, maintained, or improved. Perform regular reviews of the day-to-day procedures that may lead to errors, mistakes, account duplication, account not in appropriate context, or inactive.	X		
Report weekly on all event /incident or requests processes.	X		
Report quarterly on recommendations on ways to improve handling Incident or requests.	X		

4.2 Enterprise Command Centre ("ECC")

The ECC has various sub functions that all are part of the delivery of Data Centre Operations support. Each function is broken down, however some tasks may overlap as they relate to 7/24 shift efforts. During off hours the SP must ensure that the resources provided will be able to multi task and provide the functional support as required with the minimal amount of resources. The efforts at APDC and MCDC, will require a skeleton crew providing off hours support, predominantly with the Data Centre Tape and Facility Operations. Event Management functions will be distributed and the bulk of the Event Management will take place at KEDC, or another location in the NCR that has the majority of the resources located. The shift schedules used by the ECC and sub functions will be based on a 4 shift rotation, as they are currently. Shift schedules are subject to review and upon agreed terms, may be altered to better accommodate SSC service delivery.

4.2.1 Event Management Mainframe Function

The Service Provider must monitor and respond to the system consoles of all mainframe images, currently 46 MVS, and Linux platforms. These images reside in 3 data centres (Macdonald-Cartier, King Edward and Summerside), but are monitored from a single control centre by the Service Provider's Event Management Mainframe Team. SSC automation software must be used by the Service Provider's Event Management Mainframe Team to monitor, operate and control all images, which includes message suppression, error notification, and automated start up and shut down of online environments, and automated incident escalation by pager.

The mainframe operating system in use is Z/OS. A significant number and variety of online environments are monitored, including CICS, DB2, IDMS, Oracle, Websphere and others. Additionally, a number of internally developed applications are monitored or used by the Systems Operators.

Client images are not homogenous in terms of operating conditions and services provided, however all images are provided with a common base of services. Client images can be grouped into the following general categories:

(a) Level 1 batch support images: The Service Provider will perform the system operational duties which include but are not limited to ensuring that the system is available during scheduled hours, starting and stopping online regions at the Client's request or according to published hours of operation, and ensuring that sufficient initiators and tape drives are available to allow batch processing flow. Some imaging

support requires production control support, such as running overnight batch, first level application problem resolution, and normal base of service Functions, such as supporting online environments. In addition, some images require not only base of service duties, such as supporting online environments, but also a significant amount of involvement in problem management activities. The Service Provider must attend and participate in a daily problem review meeting; and

(b) Other Client images: These systems run common government applications such as payroll and financial control systems. The Service Provider will monitor the images, starting and stopping online regions, running batch processing at night and providing first level application incident resolution services.

The Service Provider must perform monitoring and system integrity checking: The Service Provider must monitor the operations and provide systems integrity management services, on a daily basis, to ensure that Clients' environments and information resources are available as per SSC service level targets.
Systems, networks and business applications must be monitored by the Service Provider for red flags or alerts. Incidents that are identified must be analyzed and resolved by the Service Provider in accordance with SSC Service Management process (SSC Service Management is a discipline for managing information technology IT systems based on IT Infrastructure Library (ITIL). When no satisfactory resolution can be achieved through the application of the resolution prose, in the relevant documentation, incidents must be fully documented, tracked and escalated by the Service Provider following the SSC Service Management framework of incident Records (IR). Additionally, the Service Provider must review, approve and implement Requests for Changes (RFCs) as required. Incidents and issues are closely monitored, and reported on according to incident Management procedures.
The Service Provider must perform batch processing (1st Level): Batch processing is scheduled on a daily, weekly, monthly and yearly basis through automated and manual schedules. The Service Provider must ensure these schedules are managed, executed, monitored, analyzed and maintained in order to ensure the successful completion of the various batch applications. The Service Provider must perform first level support of batch processing errors and alerts. The Service Provider must perform restores and batch reruns in order to fix problems. The Service Provider must escalate as per SSC escalation procedures, any incident that they cannot resolve to Level 2 support. The Service Provider must ensure system performance and availability are monitored and reported on a monthly basis; that system and environmental integrity are assured through continuous monitoring of consoles; and that for systems and business application alerts, the alerts are investigated and handled as per SSC Service Management guidelines.
Incidents are analyzed, documented in the SSC Service Management tools suite as Incident Records (IRs) and must be monitored and tracked by the Service Provider through the resolution process by various resolver groups and technical teams.

The Service Provider must perform Event Management Mainframe coordination: Checklists and schedules must be monitored daily and information gathered by the Service Provider in order to report to the various levels and forums. For example: WHY (What Happened Yesterday) and SoftOps Weekly Change planning. In particular, the Service Provider must maintain logs, incident and problem management systems, so that this information is available for the daily and weekly meetings. In addition, daily, weekly and monthly volume and performance statistics must be gathered, analyzed and consolidated by the Service Provider for management review and reporting. Operations and system integrity checklists must be reviewed and maintained by the Service Provider on an ongoing basis. Incident escalation and severity management activities must be conducted by the Service Provider.

The Service Provider must perform Security Administration functions on mainframe systems and applications including the creation, updating, and deletion of all user IDs, groups, and system profiles. The Service Provider must also perform password resets, permissions to

datasets and other system resources and facilities and must also identify user access requirements and build group profile structure for application access. The Service Provider must perform incident resolution and provide support for issues relating to the administration functions being performed. The Service Provider must also generate reports on a monthly basis and when requested, relating to the tasks being performed.

The Service Provider resources must interface on a regular basis with service line representatives throughout PWGSC, SSC, and Other Government Departments ("OGD"'s), as well as various support desks (e.g., Engineering and Technology Support ("ETS") 2nd Level Support, Enterprise Service Desk, Production Network Support and third level support. The Production Readiness Testing ("PRT") and Automated Batch Job Scheduling ("ABJS") teams, which will include service line support areas that can be either a Service Provider or SSC resource, are also key participants and stakeholders of Event Management Mainframe services for the staging and management of Automated Cartridge System media, and virtual tape libraries.

4.2.1.1 Event Management Mainframe Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Event Management Mainframe Activities	Service Provider	SSC	SSC Comments
Monitor console automation software and tools and take remedial action as necessary.	X		
Follow a comprehensive shift checklist ("SCL") to perform tasks.	X		
Follow incident/change management processes and approved escalation process guidelines, as appropriate.	X		
Perform security access monitoring.	X		
Run/monitor batch processing and specific images as necessary.	X		
Co-ordinate Event Management Mainframe activities including environmental facilities monitoring, disaster recovery testing, and image management; be involved in development projects; develop/maintain procedure manuals; and provide Level 1 and Level 2 support as necessary.	X		
Use common instruments of configuration management and automated and manual schedules, to maintain and complete Event Management Mainframe checklists daily to ensure the appropriate monitoring and action on business priorities.	X		
Develop and write all processes, procedures and checklists for the successful delivery of this function.	X		With input from SSC.
Maintain and follow all processes, procedures and checklists for the successful delivery of this function.	X		

4.2.2 Event Management Midrange Function

The Service Provider will be responsible for the operations of midrange virtual and physical servers. The midrange platforms encompass Hewlett-Packard ("HP"), Windows 2000 Server, Digital (DEC), PC/Servers and various Unix platforms. The Service Provider will be also responsible for the monitoring and operation of Public Key Infrastructure ("PKI") servers located at the King Edward Data Centre and Macdonald-Cartier Data Centre. The server operating systems consist of HP/MPE, VAX/VMS, Unix operating systems, and Windows 2K Server.
The Service Provider will be responsible for the general operations support which includes server management, console, network, technical and application operation support.

(a) The Service Provider must perform systems monitoring and production control: Systems and network monitoring, integrity management and production control, backup and restore of client systems are all activities the Service Provider must perform in order to ensure that client environments and information resources are continuously monitored, available and contain complete, accurate and secure business information. Systems and business applications incidents are identified, analyzed and resolved as a Level 1 support function where possible. When incidents cannot be resolved through normal Level 1 interventions, the Service Provider must fully document, track and escalate the IR through the SSC Service Management Framework.

(b) The Service Provider must perform operations coordination specific to the scope of ECC services. This includes:
   i. Impact assessments for new business;
   ii. Completion of service requests (a client request for SSC IT services) and service estimates (a client request for an estimate on SSC IT services);
   iii. Planning and implementation of service requests;
   iv. Implementation of new software or hardware;
   v. Coordination of new procedures, processes, training; and
   vi. Critical incident report (an ECC only "lessons learned" report that can be requested by the technical authority when there are operational issues or concerns) and service disruption report (an SSC wide "lessons learned" report that is produced when time to restore is not met on an SSC service) coordination.

The Service Provider must provide general operations support: This category includes all aspects of operations including server and Storage Area Network ("SAN") console and network support. The Service Provider must complete checklist items which may include verifying that databases are active. The Service Provider must monitor the job queues to minimize any bottlenecks. The Service Provider must handle system shutdowns and start-ups, including server reboots.
The Service Provider must perform technical and application operations support: The Service Provider must provide account administration. This includes the creation of new accounts, modifications, and deletion of user accounts. The Service Provider must perform modifications of batch queues, creation and deletion of batch queues, verifying database status for select SSC clients, first level troubleshooting and monthly statistical reports. Modifications to priority streams must be performed by the Service Provider as required. The Service Provider will be the team contact for clients. The Service Provider must administer technical changes and coordinate procedure implementation. The Service Provider must also provide support for various management applications such as: time recording and project monitoring system; inventory management; and Midrange Information Tracking System ("M.I.T.S."), PKI Operations and change management at KEDC (with PKI DR at MCDC).

The Service Provider must handle technical applications and ensuring that proper training is given to all Service Provider resources supporting all servers and or systems within the Event Management Midrange function. The Service Provider must make any changes to procedures and the operations checklist, and ensure that all daily activities are handled properly and escalated as required.
The Service Provider must update the corporate Configuration Management Database ("CMDB") tool.
The Service Provider must provide reporting and documentation support: The Service Provider must provide regular and ad hoc reports and must maintain report accuracy and current documentation in support of the function.
The Service Provider will be responsible for the operations of servers. This wide variety of platforms demands that the Service Provider interface directly and through intermediaries in a number of areas (e.g., with incident Management representatives of Client). In addition, the Service Provider must interface with personnel from Automated Batch Job Scheduling ("ABJS") of the Enterprise Data Centre ("EDC"). Occasionally, the Service Provider must interface with SSM and ETS Mid-Range Support Engineering.

4.2.2.1 Event Management Midrange Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Event Management Midrange Activities	Service Provider	SSC	SSC Comments
Track and monitor activities of major midrange platforms and/or clients.	X		
Monitor job and print queues.	X		
Perform system shutdowns/start-ups as needed.	X		
Implement incident and change management procedures, including escalation procedures as required.	X		
Administer security administration policies and procedures.	X		
Monitor all physical environments after regular hours.	X		
Develop and write all processes, procedures and checklists for the successful delivery of this function.	X		With input from SSC.
Maintain and follow all processes, procedures and checklists for the successful delivery of this function.	X		

4.2.3 Network Monitoring Function

The ECC Operations ensures all infrastructure equipment including network equipment is monitored and operational. Direction is provided by the support areas on what remediation, reporting, and monitoring efforts are required. ECC Operations will be responsible for verifying the SLA's for sites that are monitored when an event is raised, to ensure appropriate escalation and prioritization standards are met.

4.2.3.1 Network Monitoring Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Network Monitoring Activities	Service Provider	SSC	SSC Comments
Monitor console automation software and tools and take remedial action as necessary.	X		
Follow a comprehensive shift checklist (“SCL”) to perform tasks.	X		
Follow incident/change management processes and approved escalation process guidelines as appropriate.	X		
Coordinate networking; be involved in development projects; develop/maintain procedure manuals; and provide support as necessary.	X		
Use common instruments of configuration management and automated and manual schedules, to maintain and complete networking checklists daily to ensure the appropriate monitoring and action on business priorities.	X		
Develop and write all processes, procedures, and checklists for the successful delivery of this function.	X		With input from SSC.
Maintain and follow all processes, procedures and checklists for the successful delivery of this function.	X		
Follow all processes, procedures and checklists for the successful delivery of this function.	X		

4.2.4 ECC Tape Operations Function

The Service Provider must perform activities taking place in tape libraries located at the King Edward, Aviation Parkway, PDLC, GPC, and the Macdonald-Cartier Data Centres and is specific to the mainframe and Open Systems segments of the Data Centre Operations environment. 'Tape' is defined as the family of media consisting of tape cartridges (LTO-4, LTO-6, 3480, 3592, 3490, and 9840) and virtual storage manager (VSM) media (virtual volumes and 9840 'MVC's). The Service Provider must perform tape mounts, tape inventory management, shipping/receiving of media. The Service Provider must also maintain eCloud accounts that are maintained on a third party provider to manage tapes being shipped off to or from their premises. At this time the third party provider is Iron Mountain.

The Service Provider must support approximately 40 MVS images consisting of images for PWGSC internal clients and Other Government Department (OGD) including facilities management. The Service Provider must provide offsite vaulting services for OGDs and other clients under the disaster recovery (DR) services agreements.

The Service Provider must monitor the Virtual Storage Management (VSM) technology. While this technology reduces the amount of handling of physical media, the Service Provider must be aware of the status of the VSM and execute commands specific to the VSM. The Service Provider must ensure that a sufficient number of Multi-Volume Cartridges (MVCs) are available in the Automated Cartridge System (ACS) in order for data to be migrated from the virtual storage unit to tape. This helps ensure that sufficient space remains available in the data buffers of the Virtual Tape Storage Subsystem (VTSS).

An overview of the working environment is as follows:

a. The Service Provider must perform Service Management duties: The Service Provider must respond to Service Management requests from Product Owners, Product Holders and client representatives through scheduled events and RFC's. Device cleaning schedules must be maintained by the Service Provider and ACS Scratch forecasts must be completed by the Service Provider to ensure sufficient resources are available to carry out scheduled activities. Systems and business applications incidents are identified within Incident Records. Incident Records related to Operational Support Level 1 and 2 must be analyzed and resolved by the Service Provider when possible. If resolution is not possible within the scope of the Service Provider function, these incidents must be escalated by the Service Provider through the ITSB Service Management framework. Occasionally, external resolver groups are involved in providing assistance to the Service Provider resources in the implementation of changes and resolutions to Incident Records,
b. The Service Provider must manage and maintain the Tape Library: Automated and manual daily schedules must be extracted by the Service Provider for review and tracking of the checklist of activities that need to be performed. Automated Cartridge System (ACS) performance and availability must be monitored and reported by the Service Provider. ACS and Tape Library integrity must be assured by the Service Provider through consistent monitoring of consoles for systems and alerts. ACS system messages, automated job bill of materials (JBMs), schedules and control documentation are daily inputs reported on by the Service Provider in the performance and quality control reports. Incidents are analyzed, documented in IRs and monitored by the Service Provider through the resolution process by the various Resolver Groups and technical teams.
c. The Service Provider must manage Tape Handling: ACS messages, automated JBM's, and control documentation must be managed by the Service Provider. This is accomplished by responding to ACS Silo messages for enters and ejects, JBMs, tape mounts, scheduled or requested device cleanings and the maintenance of media inventories. The Service Provider will receive, log and store media received from clients and external storage facilities. Furthermore, the Service Provider must prepare media for shipment to clients.
d. Daily checklist, and ACS System messages must be monitored by the Service Provider and information gathered to report to various levels and forums; WHY (What Happened Yesterday) daily meeting and SoftOps (weekly Change meeting). The Service Provider must gather daily, weekly and monthly volume and performance statistics and must analyze and consolidate this data for management review and reporting. Operations and system integrity checklists must be reviewed and maintained by the Service Provider on an ongoing basis. Incident escalation and severity management activities must be conducted regularly by the Service Provider.

The Service Provider must also provide on-site services during SSC business hours at the PDLC and GPC sites. The resource must provide the same functionality as noted above. Included at this site is digitization work for the archiving of sensitive, historical media. Resources will need to work between two buildings where the digitization work is performed.

The Service Provider must gather daily checklists, schedules, print console messages, and other relevant information in order to report to various levels and forums: (WHY – What Happened Yesterday (daily) and SoftOps (weekly). Daily, weekly and monthly volume and performance statistics must be gathered, analyzed, consolidated and reported by the Service Provider. Operations and system integrity checklists must be reviewed and maintained regularly by the Service Provider. Incident escalation and severity management activities must be conducted by the Service Provider.

The Service Provider must interface with client representatives in various Operations teams, Business Integration, and Technical Coordinators. These teams represent PWGSC, LAC, and OGD clients. Occasionally the Service Provider must interface with product owners and product holders using scheduled events. External support from engineering is provided as required through the service management sub-processes of RFC and IR handling and resolution.
In special circumstances, the Service Provider must interface directly with Server Systems Management (SSM) and the Engineering & Technology Support (ETS) groups, as well as application groups, specifically for incident and change management processes. This usually occurs through RFC's, IR's and Emails with coordination provided by the SSC.

4.2.4.1 ECC Tape Operations Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Data Centre Operations Tape & Storage Activities	Services Provider	SSC	SSC Comments
Manage and maintain the tape inventory;	X		
Perform shipping/receiving activities;	X		
Meet client Service Level Objectives (SLO's) through common instruments of configuration management, automated and manual schedules and checklists which have been developed and maintained by the Contractor's Team. Checklists are completed by the Contractor's resources daily to ensure the consistent monitoring of actions on business priorities; and	X		
Develop, write, maintain and follow all processes, procedures and checklists for the successful delivery of this function.	X		

4.2.5 ECC Facilities Operations Function

In support of the facility, the service provider must also assist SSC Data Centre Facilities team for remote hands support for the IT Equipment plus help coordinate emergency repair and maintenance activities for the electrical/mechanical equipment specifically for the KEDC, MCDC and APDC locations. This also includes support for annual power maintenance shutdowns and security access support as needed for all these sites. This will also include working with the SSC Data Centre Facilities contacts to help coordinate and support routine or act as first response for onsite facility type work only on a 7/24 basis for the KEDC, MCDC and APDC locations.

4.2.5.1 ECC Facilities Operations Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Data Centre Operations Facilities Activities	Services Provider	SSC	SSC Comments
Monitor Data Centre electrical/mechanical equipment	X	X	Shared responsibility

Data Centre Operations Facilities Activities	Services Provider	SSC	SSC Comments
Perform security access monitoring.	X		
Perform shipping/receiving activities;	X		
Meet client Service Level Objectives (SLO's) through common instruments of configuration management, automated and manual schedules and checklists which have been developed and maintained by the Contractor's Team. Checklists are completed by the Contractor's resources daily to ensure the consistent monitoring of actions on business priorities; and	X		
Develop, write, maintain and follow all processes, procedures and checklists for the successful delivery of this function.	X		

4.3 Transition Services

The transitions in (from the current Service Provider) and out (to any future Service Provider) must be accomplished in a manner that is non-disruptive and well planned to accommodate the progressive takeover of the service delivery. The transition processes must minimize risk to the quality of service, and cause minimal impact to clients' operations.

4.3.1 Transition-In Plan

Within 10 calendar days of the Contract Award Date, the date of issuance of the Contract by SSC, the Service Provider must provide to SSC a Transition-In Plan ("TIP") for approval and acceptance. It must be sufficiently detailed to clearly identify how the Service Provider will transition-in all Enterprise Command Centre services from the current Service Provider. At a minimum, the TIP must include, but is not limited to:

- How the Service Provider will obtain an understanding of the Enterprise Command Centre Domains and all Functions and Sub-Functions contained within
- How the Service Provider will train and prepare their key resources so that they are fully capable of providing Services
- Identification of the Key Resource names and security classifications so site security accesses can be pre-arranged and the beginning of the submission of the résumés for the remaining Key Resources who will make up the total Key Resources to be working at the start of Transition-In activities
- ECC knowledge transfer strategy for all Key Resources and for all Service Provider resources;
- Service Provider's proposed transition schedule
- Training plans and methodology (which would include but not be limited to: shadowing with outgoing personnel, site visits, familiarization with tools, study of SSC-provided operational documentation and internal assessment methodology)
- How the Service Provider will obtain an understanding of the ECC technical environments, support structure and business relationships; and
- Reporting strategy including:
    - Weekly Transition-In Reports (including but not limited to attainment levels per training category and resource levels);
    - Weekly Operational Reports, as described in Appendix A to Annex A
    - Establishing service level reporting, as described in Appendix A to Annex A
    - Establishing quality reporting, as described in Appendix A to Annex A

- Transition-in incident reporting; reporting (including but not limited to Daily Backlog Report and Activity Plan as described in Appendix A to Annex A
- Service Provider-related escalation process/governance

The 30 calendar days immediately following the date of acceptance of the TIP is the Transition-In Period, during which the TIP must be implemented by the Service Provider. SSC will not change the technical infrastructures or environments identified in the RFP during the Transition-In Period. The Transition exercise is of critical importance to ensure that the Service Provider is fully capable of performing the responsibilities of the Function at Contract Start Date and to demonstrate to SSC that the expected levels of service are being achieved.

On the day after the date of acceptance of the TIP, the Service Provider will provide, on site, the Resources outlined in task authorization in accordance with Appendix C to Annex A – Tasking procedures, in the event that the resource proposed in the Service Provider's Proposal is unavailable through no fault of the Service Provider, a substitute approved and accepted by SSC. This substitute must meet all of the requirements associated with the category as per Appendix D to Annex A – Resource Assessment and Criteria response tables, meet the language requirement relative to the ratios identified in Section 2.4, and hold a valid security clearance at the requisite level to be accepted.

SSC will ensure that the service documentation maintained by the incumbent Service Provider will be complete, approved by SSC, and available for use by the new Service Provider upon contract award.

The Transition-In must be completed by the Service Provider within 30 calendar days following the date of acceptance of the Transition-In Plan [the "transition" – in TIP]. The Contract Start Date is the day immediately following completion of the 30-day Transition-In. At the Contract Start Date the following must have occurred:

a) The Functions must be transitioned to new Service Provider
b) The Key Resources must be autonomous in their new roles
c) The Service Provider must have provided the minimum staffing requirement of Key Resources as identified, or their equivalent as approved by SSC
d) The Service Provider must have taken full responsibility for the delivery of all Functions.

SSC will pay the Service Provider as per the Request for Proposal if all of (a) through (d) (the objectives) above have occurred.

4.3.1.1 Transition-In Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Transition-In Activities	Service Provider	SSC	SSC Comments
SSC will not change the technical infrastructures or environments during the 30-day Transition-In Period.		X	
Ensure key resources are available on a full time basis from the first day of the Transition-In Period, and for a minimum of 6 months following the end of the Transition-In Period.	X		
Ensure key resources are available to perform certain work outside of regular business hours as	X		

Transition-In Activities	Service Provider	SSC	SSC Comments
required.			
Key Resources must be made available as required by SSC, and will be expected to learn the key aspects of the Service Desk Functions from the incumbent resources during the Transition Period.	X		
Key Resources must transfer this knowledge to the winning bidder's remaining contractor resources by the Contract Start Date.	X		
The resources proposed by the winning Bidder must have the experience, skills and knowledge to perform their roles, and may require specific knowledge transfer on specific aspects of the SSC domain or systems to assume operational responsibilities.	X		
Contractor must ensure that Resource availability is maintained and that the Contractor's Transition activities do not cause service disruptions.	X		
If an equivalent resource is provided, the resource is subject to approval by SSC.	X		
Contractor must provide to the a weekly "Transition-In" report detailing the status of all "Transition-In" activities as well as transition issues, mitigation, progress, recommendations and any other pertinent details.	X		
All requirements of the Transition-In Plan must be implemented on schedule.	X		
Contractor must carry out the transition of its staff and processes associated with a Function such that it is ready and able to carry out all work associated with the Function by the end of the Transition-In Period.	X		
The Transition exercise is of critical importance, to ensure that the Contractor is fully capable of performing the responsibilities of the Function and to demonstrate to SSC that the expected levels of service are being achieved.	X		
SSC shall notify the Contractor, in writing, of acceptance of the Transition when the Contractor has demonstrated to the satisfaction of SSC that it is ready to carry out all of the work described in this SOW.		X	
All costs associated with the Transition shall be the	X		

Transition-In Activities	Service Provider	SSC	SSC Comments
responsibility of the Contractor.			

4.3.2 Transition-Out Plan

At the end of the Contract Period, the Service Provider must assist with the transition of the Domain to a new Service Provider. The Service Provider must cooperate with a new Service Provider to ensure that smooth and seamless transition of services occurs. The Service Provider must ensure that overall operational availability is not disrupted; existing service levels are maintained and Contract deliverables continue to be delivered while transition and knowledge transfer to a new Service Provider or to SSC staff occurs.

4.3.2.1 Transition-Out Responsibility Matrix

Where indicated below with an "X", the Service Provider must provide the services.

Transition-Out Activities	Service Provider	SSC	SSC Comments
Ensure that documentation is up to date and accurate. Copies of the documentation must be provided within 2 working days on written request from SSC.	X		
Ensure operational procedures are up to date and accurate.	X		
Ensure operational checklists are maintained to current requirements and are complete and accurate. Copies of these checklists must be provided within 2 business days on written request from SSC.	X		
Continue to meet established operational service levels and targets.	X		
Continue to meet existing service level targets as they relate to incident management and change management.	X		
Allocate the necessary time to assist in one-on-one knowledge transfer to the incoming Contractor.	X		
Prepare and deliver detailed transition documentation for presentation to SSC to be utilized with the incoming Contractor. The transition documentation and presentations must be provided for each Function and Sub-Function within the Request for Proposal. The documentation must describe, in the necessary detail, all the pertinent and important details necessary for a successful transition to the incoming Contractor.	X		
Prepare weekly Transition-Out reports.	X		

5 Resource Requirements

This section details the resource requirements required to perform the ECC functions.

5.1 Expected Quality

The expected approximate annual volumes for the ECC are as follows:
The expected annual volumes for ECC are approximately 47,500 configuration items, and 30,500 alerts. These volumes will need to be processed as per the SLAs using the resource numbers listed in section 5.2.

5.2 Resource Positions

Service	Function	Position Title	Qty
ECC	Event Management	ECC Event Management Team Lead	4
ECC	Event Management	Production Support Analyst	3 – MF 3 - Mid
ECC	Event Management	ECC Event Management Senior Operator	4 – MF 3 - Mid
ECC	Event Management	ECC Event Management Intermediate Operator	4 – MF 4 - Mid
ECC	Event Management	ECC Event Management Junior Operator	4 - MF 4 - Mid
ECC	IT Service Management	ITSM Senior Management Consultant	2
ECC	IT Service Management	ITSM Intermediate Management Consultant	1
ECC	Management	Operations Domain Manager	1
ECC	Management	Project Control Office Analyst	1
ECC	ECC Tape Management	ECC Senior Tape Operator	2
ECC	ECC Tape Management	ECC Intermediate Tape Operator	1
ECC	ECC Tape Management	ECC Junior Tape Operator	1
ECC	ECC Tape Management	ECC Tape Analyst	1
ECC	ECC Facilities Management	ECC Senior Facility Operator	3
ECC	ECC Facilities Management	ECC Intermediate Facility Operator	2
ECC	ECC Facilities Management	ECC Junior Facility Operator	2

5.3 Position Descriptions

5.3.1 ECC Event Management Team Lead

The ECC Event Management Team Lead is responsible for leading and supervising the Mainframe, Midrange, and Network teams, and for managing the workload and shift scheduling of Event Management resources. They liaise with supervisors and team leads of other support groups, and provide technical and process support. They provide leadership

on incidents, and ensure operations documentation is kept up to date. The Event Management Team Lead ensures any operational improvements that are identified are brought to the attention of ECC management.

5.3.1.1 ECC Event Management Team Lead must meet the following requirements

- 4 years of experience as a supervisor or team lead in mid-range, mainframe or network operations

Within the last 8 years the resource must have:

- Experience in keeping operational resources current with client technical and operational requirements and procedures
- Experience in using incident and change management processes including inputting or updating information into incident and change management systems
- Experience in project control / coordination or project management
- Experience working in a data centre environment
- Experience working with Tivoli Enterprise Systems Management tool or equivalent enterprise ITSM tool
- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 12 of the following requirements:

- Experience in using incident and change management processes including inputting or updating information into
- Incident and change management systems on 3 or more projects
- Experience in project coordination or project management on 3 or more projects
- Create, update, and implement operational procedures and/or checklists
- Monitor the performance of operations through the use of metrics
- Manage and/or coordinate incidents and/or change management as per ITIL guidelines
- Translate user requests into operational requirements
- Understanding and enforcing data centre Security procedures
- Monitor environmental systems and taking appropriate action
- Initiating / rebooting / troubleshooting Windows Server
- Initiating / rebooting / troubleshooting LINUX, UNIX
- Initiating / rebooting / troubleshooting OS390 or MVS/ESA
- System Automation tools (CA7)
- TELNET, SSH, REMOTE DESKTOP CONNECTION
- System security products (for example, SECURITY 3000, HITMAN, GUARDIAN)
- Tape Management System (MEDIA MANAGER or TMS or IBM/VTS)
- Create, update, and implement operational procedures and/or checklists on 3 or more projects
- Reading, understanding and identifying components of a network topology diagram
- Troubleshooting network related incidents

5.3.2 Production Support Analyst

Represents Operations at inter-group project meetings when new systems or workloads are being introduced. Assessment of the impact to the group to determine what procedures and processes will need to be in place for Console Operations. Analyzes problem situations, to determine chain of events, causes, and solutions to prevent reoccurrence. Coordinates role of first level support for PWGSC's Public Key Infrastructure (PKI) environment. Evaluating and approving INFOMAN change records for the operational environment. Coordinates with the Change Manager the scheduling of changes during the weekly maintenance window.

Manages the training and educational needs of the Operations group by providing other Coordinators and Shift Supervisors with input into staff skills evaluations, and identifying any skills gaps. Identifying development needs and coordinating training and education of the Operations group, both as a whole and individually. Provides project management and coordination of new initiatives, or for new workloads being brought into the environment.

5.3.2.1 Production Support Analyst must meet the following requirements

- 4 years' experience administering operations
- 4 years' experience in coordinating and assisting with the incident and/or change management in an operational environment
- 4 years' experience in managing training and educational needs of the operations group
- 4 years' experience in project coordination
- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 15 of the following requirements:

- Create, update, and implement operational procedures and/or checklists
- Monitor the performance of operations through the use of metrics
- Experience in using incident and change management processes including inputting or updating information into incident and change management systems on at least 3 projects
- Project management
- Experience working with Tivoli Enterprise Systems Management tool or equivalent
- Initiating / rebooting / troubleshooting OS390 or MVS/ESA
- Initiating / rebooting / troubleshooting Windows Server
- Initiating / rebooting / troubleshooting LINUX, UNIX
- Console Utilities & Diagnostic Tools (MVS/JES2, TSO/ISPF, IOF/SDSF)
- At least 2 of the following: CLISTS, JCL, SYSLOG, LOGREC, DUMPS
- System Management Tools (for example, WHATSUP PRO)
- System Automation (CA-7)
- At least 2 of the following: AF/OPERATOR, OPS/MVS, AUTOMATE X/C, AUTOMATION POINT, SA/390
- Security Systems (for example, TOP SECRET, RACF, AOF OPERATOR)
- Online Regions (CICS, DBS, IDMS, WEBService ProviderHERE)
- Monitoring (for example, OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)
- Tape Management System (MEDIA MANAGER or TMS or IBM/VTS)
- Reading, understanding and identifying components of a network topology diagram
- Troubleshooting network related incidents

5.3.3 ECC Event Management Senior Operator

The Event Management Senior Operator is responsible for in depth support of operating server systems including performing DASD dumps, and system IPLs. They must perform first and second level troubleshooting for server, mainframe, network, batch processing and IT infrastructure related incidents. They are responsible for analyzing Problems and incidents to determine root cause and assist in providing solutions to prevent reoccurrence. They must monitor mainframe, server and network systems and console software and utilities. They must also update and maintain operational documentation and procedures. The main objective of the Senior Operator is to provide guidance and direction for the intermediate and junior operators and triage more complex incidents and event management issues.

5.3.3.1 ECC Event Management Senior Operator must meet the following requirements

- 4 years working in IT Operations in a data centre environment

Within the last 8 years, the resource must have:

- Experience in mainframe, server or network system monitoring
- Experience in batch processing
- Experience in using incident and Change management processes including inputting or updating information into event, incident and change management systems
- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 13 of the following requirements:

- Operate mainframe, server computers, or networking infrastructures
- Experience in mainframe and server system monitoring on 4 or more projects or engagements
- Experience in using Event, incident and Change management processes including inputting or updating information into event, incident and change management systems on 4 or more projects
- Experience in mainframe batch processing on 4 or more projects
- Monitor data centre environmental systems
- Create, update, and implement operational procedures and/or checklists
- Experience in using system performance or diagnostic tools
- Initiating / rebooting / troubleshooting Windows Server
- Initiating / rebooting / troubleshooting LINUX, UNIX
- Initiating / rebooting / troubleshooting OS390 or MVS/ESA
- System Management Tools (for example, WHATSUP PRO)
- Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)
- Online Regions (CICS, DB2, IDMS, WEBSPHERE)
- Batch Processing (CA-7, CONTROL-M, TWS)
- Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)
- Communication tools (Telnet, or Remote Desktop Connection, or equivalent)
- Tape Management Systems (CONTROL-T or ZARA or RMM or TSM) or equivalent
- Reading, understanding and identifying components of a network topology diagram
- Troubleshooting network related incidents

5.3.4 ECC Event Management Intermediate Operator

The Event Management Intermediate Operations is responsible for operating server systems including performing DASD dumps, and system IPLs. They must perform first level troubleshooting for server, mainframe, network, batch processing and IT infrastructure related incidents. They are responsible for assisting in analyzing Problems and incidents to determine root cause and assist in providing solutions to prevent reoccurrence. They must monitor mainframe, server and network systems and console software and utilities. They must perform tape backup operations including verifying backup status and entering / ejecting tapes from tape library. They must perform print operations that includes running print jobs and packaging for shipment to clients. They must also update and maintain operational documentation and procedures.

5.3.4.1 ECC Event Management Intermediate Operator must meet the following requirements

- 2 years working in IT Operations in a data centre environment

Within the last 8 years, the resource must have:

- Experience in mainframe, server or network system monitoring
- Experience in batch processing
- Experience in using incident and Change management processes including inputting or updating information into incident and change management systems
- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 13 of the following requirements:

- Operate mainframe or server computers
- Experience in mainframe and server system monitoring on 2 or more projects or engagements
- Experience in using Event, incident and Change management processes including inputting or updating information into incident and change management systems on 2 or more projects
- Experience in mainframe batch processing on 2 or more projects
- Monitor data centre environmental systems
- Create, update, and implement operational procedures and/or checklists
- Experience in using system performance or diagnostic tools
- Initiating / rebooting / troubleshooting Windows Server
- Initiating / rebooting / troubleshooting LINUX, UNIX
- Initiating / rebooting / troubleshooting OS390 or MVS/ESA
- System Management Tools (for example, WHATSUP PRO)
- Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)
- Online Regions (CICS, DB2, IDMS, WEBSPHERE)
- Batch Processing (CA-7, CONTROL-M, TWS)
- Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)
- Communication tools (Telnet, or Remote Desktop Connection, or equivalent)
- Tape Management Systems (CONTROL-T or ZARA or RMM or TSM) or equivalent
- Reading, understanding and identifying components of a network topology diagram
- Troubleshooting network related incidents

5.3.5 ECC Event Management Junior Operator

The Event Management Junior Operator is responsible for operating server systems including performing DASD dumps, and system IPLs. They perform first level troubleshooting for server, mainframe, network, batch processing and IT infrastructure related incidents, and monitor mainframe and server systems and console software and utilities. They are responsible for performing tape backup operations including verifying backup status and entering / ejecting tapes from tape library.

5.3.5.1 ECC Event Management Junior Operator must meet the following requirements

- 1 year working in IT Operations in a data centre environment

Within the last 8 years, the resource must have:

- Experience in mainframe, server or network system monitoring
- Experience in using incident and Change management processes including inputting or updating information into
- Incident and change management systems

- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 5 of the following requirements:

- Operate mainframe or server computers on 2 or more client engagements
- Initiating / rebooting / troubleshooting Windows Server or LINUX or UNIX or OS390 or MVS/ESA
- System Management Tools (for example, WHATSUP PRO)
- Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)
- Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)
- Tape Management Systems (CONTROL-T or ZARA or RMM)
- Reading, understanding and identifying components of a network topology diagram
- Troubleshooting network related incidents

5.3.6 ITSM Senior Management Consultant

The ITSM Senior Management Consultant is responsible for providing senior level expertise and guidance to support to the IT Service Management environment at SSC in one or more of the following areas: Event Management, Incident Management, Problem Management, IT Service Desk, Configuration Management, Change Management, Release Management, Security Operations Management, IT Service Continuity Management, Capacity Management, Availability Management, Service Management, IT Financial Management. They oversee and manage the creation, modification and updating of IT Service Management documentation, processes and procedures, and lead or manage IT Service Management projects. They must conduct IT Service Management briefings and presentations to SSC management and other support groups, and liaise with SSC management to provide strategic guidance and recommendations on IT Service Management business. They are responsible for ongoing support activities associated with the maintenance of International Organization for Standards (ISO) certification, and must participate in projects related to ISO certification.

5.3.6.1 ITSM Senior Management Consultant must meet the following requirements

- 4 years of experience in operations management consulting

Within the last 8 years, the resource must have:

- ITIL Intermediate Certificate in IT Service Management (ITIL v3, at least one ITIL Intermediate Module)
- Experience in planning IT Service Management (ITIL) implementations in a large data centre environment
- Experience in communicating plans and strategies to management and employees
- Experience in leading the implementation of IT Service Management (ITIL) projects
- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 6 of the following requirements:

- Analysing operational statistics on at least 5 projects
- Working with service management tools (e.g. Infoman; Tivoli, etc.)
- Working with IT Service Management (ITIL) tools or systems in a data centre production environment on 3 or more projects
- Working as a Project Manager on at least 3 IT Service Management projects
- Developing procedures for IT Service Management (ITIL) on at least 3 projects
- Creating and updating data flow diagrams using Visio or equivalent flowcharting tool

- Providing training to IT personnel on 3 or more projects
- Experience in planning IT Service Management (ITIL) implementations in a large datacentre environment on at least 3 or more projects
- Experience in communicating plans and strategies to management and employees on at least 3 or more projects

5.3.7 ITSM Intermediate Management Consultant

The ITSM Intermediate Management Consultant provides support to the IT Service Management environment at SSC in one or more of the following areas: Event Management, Incident Management, Problem Management, IT Service Desk, Configuration Management, Change Management, Release Management, Security Operations Management, IT Service Continuity Management, Capacity Management, Availability Management, Service Management, and IT Financial Management. They must create, modify and update IT Service Management documentation, processes and procedures, and must manage or participate in IT Service Management projects. They must conduct IT Service Management presentations to other support groups, and must provide ongoing support activities associated with the maintenance of International Organization for Standards (ISO) certification. They must participate in projects related to ISO certification.

5.3.7.1 ITSM Intermediate Management Consultant must meet the following requirements

- 3 years of experience in operations management consulting

Within the last 8 years, the resource must have:

- ITIL Intermediate Certificate in IT Service Management (ITSM) (ITIL v3, at least one
- ITIL Intermediate Module)
- Experience in planning IT Service Management (ITIL) implementations in a large data centre environment
- Experience in communicating plans and strategies to management and employees
- Experience in the implementation of IT Service Management (ITIL) projects
- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 7 of the following requirements:

- Analyzing operational statistics on at least 3 projects
- Working with service management tools (e.g. Infoman; Tivoli, etc.)
- Working with IT Service Management (ITIL) tools or systems in a data centre production environment
- Working as a team member on at least 3 IT Service Management (ITIL) projects
- Developing procedures for IT Service Management (ITIL) disciplines
- Creating and updating data flow diagrams using Visio or equivalent flowcharting tool
- Providing training to IT personnel
- Experience in planning IT Service Management (ITIL) implementations in a large data centre environment
- Experience in communicating plans and strategies to management and employees
- Creating and updating operational documentation

5.3.8 Operations Domain Manager

The Operations Domain Manager manages the day-to-day operation of a designated Function(s) or responsibility area. They are the single point of contact for day-to-day service

delivery within responsibility area, and are responsible for the performance, service quality and customer satisfaction of the services delivered within a designated Function(s) or responsibility area. They identify and implement opportunities to improve service and reduce cost, and ensure all service delivery commitments are met or exceeded. They must provide leadership, direction, and technical support to a designated Function(s) or responsibility area.

5.3.8.1 Operations Domain Manager must meet the following requirements

- 5 years of management experience in IT service delivery in a data centre environment

Within the last 8 years, the resource must have:

- Experience analyzing and re-engineering existing business processes to optimize IT operations
- Experience in developing and monitoring high level plans, policies and guidelines
- Experience communicating IT operational plans and strategies with technical staff, nontechnical staff and senior management in written and oral presentation formats
- Experience managing an IT support team of at least 15 resources for a continuous period of at least 1 year
- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 7 of the following requirements:

- Manage complex IT operations environments (multiple software and hardware platforms) on at least 2 projects
- Manage hardware, software and/or service integration
- IT project management on at least 3 projects
- Provide advice and guidance on the mapping of business to operational requirements
- Provide advice, guidance and document recommendations for modifying or implementing service delivery programs
- ITIL Foundation certification (v.2 or higher)
- IT service cost estimating related to IT operations service support and delivery
- Architecting or designing IT solutions
- Recommending and implementing process improvements or cost savings solutions in an IT operations environment
- Experience working with Treasury Board Enhanced Management Framework (EMF)

5.3.9 Project Control Office Analyst

The Project Control Office Analyst must ensure all service level commitments and deliverables are met, and that all management processes meet or exceed Client expectations. They are responsible for tracking and reporting on all ECC projects, and for gathering and reporting on all Contract performance metrics and statistics. They create and maintain all Contract documentation, create and administer the Contract documentation library and document control, and create, update and maintain all required Contract personnel documentation and records.

5.3.9.1 Project Control Office Analyst must meet the following requirements

- 4 years of IT project control experience

Within the last 8 years, the resource must have:

- Document management in an IT enterprise environment
- Valid Canadian Federal Government Security Clearance: Secret

The resource must meet at least 6 of the following requirements:

- Create and update IT operational procedures, IT performance metrics and key indicator metrics for consistency, accuracy and completeness on 2 or more projects
- Using automated tools for statistical analysis
- Monitor Work results against plans through the use of metrics (key performance metrics, key performance indicators, quality metrics, workload metrics, and metrics reporting) on 2 or more projects
- Experience in using Event, incident and Change management processes including inputting or updating information into incident and change management systems on 2 or more projects
- Coordinate and/or update contractual documentation on 2 or more projects
- Produce monthly management and statistical reports
- ITIL Foundation certification (v.2 or higher)
- Implementing document management procedures on 2 or more projects
- Office Products (MS Word or Lotus WordPro and MS Excel or Lotus 123)

5.3.10 ECC Tape Operators

In addition to having ECC Event Management responsibilities, The Tape Operator must possess experience in the various aspects of tape management. For the specified Tape Operator positions these responsibilities must be fulfilled. Tape Operator positions required for KEDC, APDC, MCDC, GPC, and PDLC.

5.3.10.1 ECC Tape must meet the following requirements

The requirements must include the following:

1. Tape handling
- Tape checkouts from tape libraries
- Tape checkins to tape libraries
- Prepare tapes for shipping to offsite vaulting
- Confirm tapes returning from offsite vaulting
- Generate offsite vaulting lists weekly
- Generate list of tapes to return from offsite vaulting weekly
- Confirm tapes going to offsite vaulting are handed off to appropriate vendor/courier service
- Assist Backup groups with ad hoc tape check in and check out services
- Serve as primary contacts for all offsite vaulting contracts
- Issue ad hoc recalls for offsite tapes if/when required
- Ensure all tapes are labelled in accordance to SSC standards
- Arrange for destruction/degaussing of damaged and/or unused tapes in accordance with SSC requirements
- Arrange for the replacement of any damaged tapes with tape vendors, where possible.

2. Tape inventory
- Confirm complete inventory of all tapes – offsite, onsite and cleaning tapes – is accounted for on a regular basis
- Provide tape inventory reports on a monthly basis for all locations

3. Backup Service Monitoring
- Monitor the backup infrastructure at each data center using backup monitoring portal supplied by SSC
- Notify 3rd Level Backup team of any issues or warnings logged on the backup monitoring portal

- Provide onsite assistance if/when vendors are required to be onsite in the event of a call home against any part of the backup infrastructure
- Use Service Management tools to log all issues and escalate when required.

5.3.11 ECC Tape Analysts

In addition to having ECC Event Management responsibilities, The Tape Analyst must possess experience in the various aspects of tape management. This position will require in-depth Tape Analysts experience in order to work with the other team members and provide direction. This position will also require the need to meet with the Tape and Storage Support teams in order to ensure the proper SSC direction is provided to the Operators. For the specified Tape Analyst position these responsibilities must be fulfilled.

5.3.11.1 ECC Tape Analyst must meet the following requirements

The requirements must include the following:

- Perform Problem and Library Management
- Perform Analysis and research on existing and new library processes
- Provide co-ordination of media library projects and activities between data centres operations and software support
- Produce reports for Management, Software Support and Clients
- Perform Library troubleshooting, problem solving and client support functions related to the Tape Media Libraries
- Team with 2nd and 3rd level support groups to resolve problems
- Monitor Media Holdings and Media Movement on a Monthly basis for trends
- Monitor Print Inventory Supplies and order supplies on a monthly basis.
- Provide DCO input for New Business to Management
- Provide DCO input to PWGSC Management for current and new business
- Maintain Tape Library procedures by creating and updating accordingly
- Monitor Tape Media across 4 data centres for integrity
- Provide Training and Support for operations and library staff at all data centres
- Ensure my backup is current on issues pertaining to DCO roles and responsibilities
- Ensure Tape Media reference tables are current with present environment
- Maintain datasets referenced to execute daily jobs to ensure integrity of databases
- Provide 1st level support to SSDC staff pertaining to Tape Media and Processes.
- Opening/updating problem tickets in InfoMan for Tape Media problems.
- Follow all procedures as outlined in job procedures, resources and applications.
- Follow specific instructions, which the client has requested for their end users.
- Creation, reviewing and maintaining operational procedures.

5.3.12 ECC Facility Operators

In addition to having ECC Event Management responsibilities, The Facilities analyst must possess experience in the various aspects of environmental management. . For the specified Facility Operator positions these responsibilities must be fulfilled.

5.3.12.1 ECC Facility must meet the following requirements

The requirements must include the following:

- Monitoring Environmental status of Data Centres.
- Performing server reboots as requested by 2nd level engineering.
- Monitor the mainframe via the system monitor consoles, use automated tools such as CA-7, CONTROL-M, and Tivoli Workstation (TWS), and perform walk-a-rounds to confirm the data centre environment is stable.

- Monitor server systems via the system monitoring console, automated tools and perform walk-a-rounds to confirm the data centre environment is stable.
- Monitor environmental systems in the data centres.
- Respond to critical data centre environmental system issues such as water on the computer room floor, fire, loss of power, or loss of air-conditioning units.
- Perform troubleshooting incidents by investigating, identifying, and resolving first level incidents with servers, tape drives and the data centre environment.
- Provide on-site escorting of vendors and SSC support personnel.

5.4 ECC and Direct Operations

Enterprise Command Centre
The resources under this contract are required to meet the objectives provided by the service lines and SSC's Customers to ensure requirements are met.

ECC Event Management
ECC Event Management must provide services that meet SSC service levels as defined by the various Customers. The level of service is dependent on the Customer and the service lines and, depending on how critical the service is, will dictate the level of work effort required to mitigate the impacted service. The Operations Domain Manager is responsible for all areas of event management to ensure Customer and service line requirements are met. The Production Support Analyst and ITSM resources ensure work activities and instructions are provided for the 7/24 operators. The 7/24 operators are responsible for ensuring all work activities are conducted and SSC priorities are addressed.

ECC Tape Management
ECC Tape Management is responsible for ensuring tape equipment is in full working order and tapes are loaded and unloaded in a manner that won't adversely affect the duration of backups. These resources must also ensure all backup scripts are run and monitored for completion. Direction and instructions will be given to the resources by the Tape and Storage service line to ensure Customer requirements are understood. The resources will manage tape accounts with third party vendors in support of the movement of tapes to offsite facilities. These cloud accounts must be kept up to date and the resources must ensure any issues are reported back to the Tape and Storage service line as soon as the issues are noted. For the work that will be done at PDLC, which is digitization backup and restore, the business Customer requires the requested tasks to be completed promptly in order not to delay backup schedules. Resources must ensure any task requested as "normal" is completed within a 5 day period. Any task requests noted as "urgent" is completed within 48 hours.

ECC Facilities Management
ECC Facilities Management will receive alarms/events via multiple monitored systems. Each system may have their own type of alarm, which can be an audible alarm, event on screen, page out and also a physical visual of an impending failure. In order to mitigate a potential failure or incident, it is critical that the resource on site conducts routine physical inspections based on set time schedules. These schedules will be provided by the facility area responsible for those data centres. Any resource that is made aware of an alarm/event, by either method noted above, must action it within 15 minutes upon notification. It is critical to ensure mitigation or resolution is executed in a timely manner as the impact to the data centre could be extensive.

APPENDIX A TO ANNEX A
Reporting Requirements and Documentation

End User Service Desk and Enterprise Service Desk

1. Documentation Requiring Annual Maintenance

a. Functional Specific Documentation (FSD)

The FSD documents the scope of the work, the influencing factors, the functional relationships, workload metrics and documentation utilized. This document provides a vehicle to assist SSC in interfacing with the service provider. The service provider must update the FSD as necessary or at a minimum of every three months and forward to the appropriate Manager for approval and distribution within SSC. The document is an all-encompassing overview of the details of the Service Desk contract. It includes, but may not be limited to, the following:

- Service Desk Scope and Description
- Service Provider/ Service Desk Organization Chart
- Governance Model
- Service Desk Functional Description
- Service Desk Relationships Diagram
- Resourcing Plan
- Reporting Requirements
- Service Desk Service Responsibility Matrix
- Communication Protocol
- Service Desk Documentation
- Shift Coverage
- Service Desk Contractual Deliverables
- SLA and Priority Matrix

This document requires an quarterly review, modification, SSC approval and sign off on an quarterly basis.

b. General Management Documentation (GMD)

This document describes the service provider's organization relative to the Service Desk contract, the roles and responsibilities of the key personnel, the service provider's management escalation process, management processes, communication plan and interaction or interdependencies between the service provider's managed functions and other Domains and SSC.

The service provider must update the General Management Documentation quarterly and forward to the appropriate Service Desk Manager for approval and distribution to SSC Management.

This document requires an quarterly review, modification, SSC approval and sign off on an quarterly basis.

2. Documentations Requiring Regular Maintenance

a. **Weekly Operational Efficiency Report**

The service provider must continuously look for ways to improve operational efficiency. The service provider will achieve this by monitoring overall performance and delivery of service and report this through key performance indicators and metrics by agent and at the desk level (i.e. occupancy, utilization, productivity, schedule adherence, etc.). This report must also identify the actions planned and taken to improve overall efficiency and operational effectiveness. Examples include recommendations to improve

FCR, reduce attrition, workforce schedule changes to improve coverage, and addressing agent performance outliers.

b. Daily Snapshot

Provide the following information from the previous day separated by Line of Business and/or by Supported Department (where applicable)

Call and Incident Management metrics include, but are not limited to, the following:

- Calls Offered
- Calls Answered
- Number of Abandoned Calls
- Percentage of utilization
- Percentage of Abandoned Calls
- Percentage of Calls Answered within target for previous day
- Percentage of Calls Answered within target for the month to date
- Average Call Talk Time
- Average Call Handle Time
- Number of Emails received
- Number of Self-Service request received (ESD)
- Number of External ticket received(ESD)
- Number of Voicemails received
- Number of Tickets Opened
- Number of Tickets Resolved at First Contact (EUSD)
- Percentage of Tickets Resolved at First Contact (EUSD)
- Incident Management ticket volume by type/category
- Root Cause Analysis for high call volume periods
- Number of Agents

Request Fulfilment

- Requests Received
- Requests Processed
- Requests to be Processed at Start of Business
- Requests to be Processed at End of Business
- Request volumes by type/category
- Number of Agents
- Percentage of utilization

Timeline: Sent next business day

c. Weekly Status Report

Provide the following information from the previous week separated by Line of Business and/or by Supported Department (where applicable). Metrics include, but are not limited to, the following:

- Call, Service request, incident and change request statistics for all End User and Enterprise Service Desks
- Percentage of Abandoned Calls
- Percentage of Calls Answered within target for previous week
- Percentage of Calls Answered within target for the month to date
- Average Call Talk Time
- Average Call Handle Time
- Number of Emails received
- Number of Self-Service request received (ESD)
- Number of External ticket received (ESD)
- Number of Voicemails received
- Number of Tickets Opened

- Number of Tickets Resolved at First Contact (EUSD)
- Percentage of Tickets Resolved at First Contact (EUSD)
- Incident Management ticket volume by type/category
- Root Cause Analysis for high call volume periods
- Number of Agents

Request Fulfilment

- Requests Received
- Requests Processed
- Request volumes by type/category
- Root Cause Analysis for periods of high backlog
- Number of Agents

Timeline: Sent the Tuesday following the completion of the reporting period

d. Bi-Weekly Quality Measurement

Provide results of Quality Review results for Request Fulfilment, Service Requests, and Incident tickets with the following information separated by Line of Business and/or Supported Department (where applicable). Metrics include, but are not limited to, the following:

- Total Number of Tickets Reviewed per agent
- Type of ticket reviewed
- Number of Reviews receiving a passing score
- Number of Reviews receiving a failing score
- Percentage of passing reviews
- Areas requiring improvements and action plan to resolve issues
- Root Cause Analysis for high rates of failure

Timeline: Sent Tuesday following the end of the reporting period

e. Monthly: Status Reports by Desk/Client; Issue Report; ACDA; T&IA

Provides the following information from the previous month separated by Line of Business and/or by Supported Department (where applicable). Metrics include, but are not limited to, the following:

Call and Incident Management

- Quality Assurance average score by Agent
- Calls Offered
- Calls Answered
- Number of Abandoned Calls
- Percentage of Abandoned Calls
- Percentage of Calls Answered within target for the month
- Average Call Talk Time
- Average Call Handle Time
- Number of Emails received
- Number of Self-Service request received (ESD)
- Number of External ticket received (ESD)
- Number of Voicemails received
- Number of Tickets Opened
- Number of Tickets Resolved at First Contact (EUSD)
- Percentage of Tickets Resolved at First Contact (EUSD)
- Incident Management ticket volume by type/category
- Root Cause Analysis for high call volume periods
- Issues impacting delivery of service

- Number of Agents

Request Fulfilment

- Requests Received
- Requests Processed
- Request volumes by type/category
- Root Cause Analysis for periods of high backlog
- Number of Agents

Timeline: Sent the 3rd business day following the completion of the reporting period

Service Delivery Issues Report
Report on current staffing and service delivery issues that are being experienced and action plan to resolve these issues with timelines for tracking.
Timeline: Provided on monthly basis for discussion during meetings with Service Provider and SSC.

ECC Reporting and Documentations Requirements

1) Reporting

Most of the reporting required is to substantiate rolled up reports and metrics. These reports are an example of what the Service Provider (SP) will need to create for work activities done by the 7/24 operators. This will provide the justification for work effort requirements during shifts and metrics that can be tracked as Key Performance Indicators (KPI's). It will also provide SSC with a tracking mechanism of amount of events, incidents, and changes that are processed on a weekly/monthly basis. These reports are subject to change at any given time based on the SP requirements and those of SSC. SSC will have the right to add reports as required to meet operational requirements.

a) Daily

- Summary of previous day issues and tasks, tracking of IR's, and RFC's that impact ECC
- Daily shift log of significant activities
- Summary of downed servers not meeting SLA's displayed in OpenNMS
- Summary of mail backup IR's and alerts
- Tally of preservation work, manual IR's, and RFC's for the month
- Total # of OPMS/MVS incidents by LPAR
- Number jobs verified, # of interventions automated & manual, and the total DASD dumps
- Number of adhoc requests performed on behalf of service areas
- Tracking of media entering or exiting the data centre
- Number of media creates per system LPAR

b) Weekly

- Summary of previous months IR's per service as specified by SCC
- Inventory for TISO SAN tapes

c) Bi-Monthly

- Summary of OA servers for SOG area

d) Monthly

- Inventory of servers and service levels for each
- Summary of work effort performed the previous month
- Summary of previous months IR's per service as specified by SCC
- Summary of issues and involvement for the month
- Breakdown of work effort provided for LAC
- SAN tape counts and summary of 3592 cleaning carts
- MCDC access list for staff
- Mainframe Metrics
- Overall LPAR availability
- Summary for all mainframe issues
- Automated and manual tape activity
- Summary of tape media holdings for MCDC and KEDC
- List of any media entering or exiting data centres

e) ADHOC

- SSC will request point in time reviews of work effort, which will require reports from all areas on the specific work being accomplished and how much time it takes to complete. This may be done 2-3 times a year to ensure SSC has an accurate account of work effort based on various times of the year, such as summer months, end of fiscal, holiday seasons, etc..
- SSC clients on occasion will request their specific service to be tracked and reported on to confirm workload and if potential issues are happening. Most times it is due to a new service or

where abnormal events or incidents are occurring. At times it may also be due to a critical service with higher visibility.

2) Documentation

The service provider must ensure that all documentation is current and accurate for all procedures and work instructions for the various services supported by the ECC. This must include specific work instructions for the shift operators on what steps to take for specific services, to mitigate events and incidents. This will require consultation with service line clients that will provide the direction and actions to be taken, including the escalation procedures. Shift operators will need to verify accuracy of documentation when addressing events or issues and update documentation as needed. Day personnel will also need to make changes based on direction from the service line areas as a result of meetings, project reviews, new changes, etc..

APPENDIX B TO ANNEX A
SSC ENTERPRISE SERVICE DESK, END USER SERVICE DESK, ENTERPRISE COMMAND CENTER AND DATA CENTER OPERATION SERVICE LEVEL AGREEMENT

(see Appendix B to Annex A pdf attachment)

APPENDIX C TO ANNEX A
TASK AUTHORIZATION PROCEDURES
(Upon Contract Award)

1. TA Request

(a) Where a requirement for a specific task has been identified and a TA is to be provided to the Contractor in accordance with the allocation methodology described in the Contract Article titled "Task Authorization", a TA Form, as attached at Appendix B to Annex B, will be prepared by the Technical Authority and sent to the Contractor.

(b) A TA Form will contain the following information, if applicable:

(i) a task number;
(ii) the details of any financial coding to be used;
(iii) the date by which the Contractor's response must be received by the Contract Authority;
(iv) a brief statement of work for the task identifying the resource category(ies), level and specialty required and describing the activities to be performed including any deliverables;
(v) the interval during which the task is to be carried out (beginning and end dates);
(vi) the number of person-days of effort required;
(vii) the specific work location; and
(viii) any other constraints that might affect the completion of the task.

2. TA Quotation

(a) Once it receives the TA Form, the Contractor must submit a quotation to the Contract Authority, identifying its proposed resources and detailing the cost and time to complete the task(s). The quotation must be based on the rate(s) set out in the Contract. The Contractor will not be paid for providing the quotation or for providing other information required to prepare and issue the TA. The Contractor must provide any information requested by Canada in relation to the preparation of a TA within 5 working days of the request.

(b) For each proposed resource the Contractor must supply:

(i) A resume and completed Appendix C to Annex A for the Category(ies) of Personnel and level(s) identified in the TA Form. The Contractor's quotation must demonstrate that each proposed resource meets the mandatory requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). With respect to the proposed resources:

(A) Proposed resources may be employees of the Contractor or employees of a subcontractor, or these individuals may be independent contractors to whom the Contractor would subcontract a portion of the Work.

(B) For educational requirements for a particular degree, designation or certificate, Canada will only consider educational programmes that were successfully completed by the resource by the time of bid closing. For post secondary education, Canada will only accept credentials from institutions recognized by the Department of Education of any Canadian province, or for those obtained in a foreign country, by either of the credential assessment organizations listed on the Website: http://www.cicic.ca/

(C) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of bid closing and must continue, where applicable, to be a member in good standing of the profession's governing body throughout the evaluation and Contract Period.

(D) For work experience, Canada will not consider experience gained as part of an educational programme, except for experience gained through a formal co-operative programme at a post-secondary institution.

(E) For any requirements that specify a particular time period (e.g., 2 years) of work experience, Canada will disregard any information about experience if the individual's resume does not include the relevant dates for the experience claimed (i.e., the start date and end date).

(F) For work experience to be considered by Canada, the Contractor's response must not simply indicate the title of the individual's position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. In situations in which a proposed resource worked at the same time on more than one project, only one project will be counted toward any requirements that relate to the individual's length of experience.

(ii) The following security information:

SECURITY INFORMATION	CONTRACTOR TO INSERT DATA
Name of individual as it appears on security clearance application form	
Level of security clearance obtained	
Validity period of security clearance obtained	
Security Screening Certificate and Briefing Form file number	

(iii) Certifications at Appendix D to Annex A (as applicable).

(c) The quotation must be submitted to the Contract Authority within the time for response identified in the TA Form. The Contractor will be given a minimum of 48 hours turnaround time to submit a quotation.

3. Resource Assessment

(a) Each proposed resource will be assessed for compliance with the mandatory requirements identified in Appendix C to Annex B applicable to that Category of Personnel. Proposed resources that do not comply with each and every mandatory criteria will not be accepted.

(b) Canada reserves the right to request references from the Contractor to conduct a reference check to verify the accuracy of the information provided. If references are requested, Canada will conduct the reference check in writing by e-mail (unless the contact at the reference is only available by telephone). A Contractor will not be responsive to a mandatory requirement unless the response is received to an e-mail reference check request within 5 working days. On the third working day after sending out the e-mails, if Canada has not received a response, Canada will notify the Contractor by e-mail, to allow the Contractor to contact its reference directly to ensure that it responds to Canada within 5 working days. Wherever information provided by a reference differs from the information supplied by the Contractor, the information supplied by the reference will be the information evaluated. The mandatory requirement will not be considered met if the reference customer is not a customer of the Contractor itself (for example, the customer cannot be the customer of an affiliate of the Contractor). Nor will the mandatory requirement be met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Contractor. Crown references will be accepted.

4. TA Acceptance

(a) Once the Contractor's quotation has been accepted by the Technical Authority, the TA Form will be signed by Canada and provided to the Contractor for signature. Whether or not to approve or issue a TA is entirely within Canada's discretion.

(b) The TA Form must be appropriately signed by Canada prior to commencement of any work. The Contractor must not commence work until a fully signed TA Form has been received, and any work performed in its absence is done at the Contractor's own risk.

APPENDIX D TO ANNEX A
EXAMPLE: Task Authorization Request and Acceptance Form
Sigma/P2P Task Authorization form will be accepted as well.

TASK AUTHORIZATION (TA) FORM			
CONTRACTO		CONTRACT NUMBER:	
COMMITMEN		FINANCIAL CODING:	
TASK NUMBER		ISSUE DATE:	RESPONSE REQUIRED BY:
1. STATEMENT OF WORK (WORK ACTIVITIES AND DELIVERABLES): SEE ATTACHED FOR STATEMENT OF WORK AND CERTIFICATIONS REQUIRED.			
2. PERIOD OF SERVICES:	FROM (DATE):	TO (DATE):	
3. WORK LOCATION:			
4. TRAVEL REQUIREMENTS:			
5. LANGUAGE REQUIREMENTS:			
6. OTHER CONDITIONS/CONSTRAINTS:			
7. LEVEL OF SECURITY CLEARANCE REQUIRED FOR THE CONTRACTOR' PERSONNEL:			

RESOURCE CATEGORY	NAME OF PROPOSED RESOUR	PWGSC SECURITY FILE NUMBER	PER DIEM RATE	ESTIMATED # OF DAYS	TOTAL COST
				ESTIMATED COST	
				GST	
				TOTAL LABOUR COST	
				ESTIMATED TRAVEL COST (IN ACCORDANCE WITH	
				TOTAL ESTIMATED COST	

8. SIGNING AUTHORITIES:		
Name, Title and Signature of Individual Authorized to Sign on Behalf of Contractor	Contractor (signature)	Date:
Name, Title and Signature of Individual Authorized to Sign on Behalf of SSC – PVR (Technical Authority)	SSC-PVR (signature)	Date:
You are requested to sell to her Majesty The Queen in Right of Canada, in accordance with the terms and conditions set out herein, referred to herein, or attached hereto, the services listed herein and in any attached sheets at the price set out thereof.		

APPENDIX E TO ANNEX A

RESOURCE ASSESSMENT CRITERIA AND RESPONSE TEMPLATES

(TO BE USED WHEN THE CONTRACT IS AWARDED)

D1.0 Task Authorization (TA) Initiation

Where a requirement for a specific task has been identified a TA will be provided to the Contractor. The qualifications and experience of the proposed resources will be assessed against the requirements set out in the below tables to determine each proposed resources compliance with the criteria identified in Section D.2 of this Annex.

D1.I Assessment

The qualifications and experience of the proposed resources will be assessed against the requirements set out in the appropriate category and level below.

D.1.2 Acceptance

Once the TA Technical Authority has accepted the quotation, the TA will be signed by the Contracting Authority and provided to the Contractor for signature. All TA Forms will be signed by the Contracting authority final approval.

D2.0 RESOURCES ASSESSMENT CRITERIA AND RESPONSE TABLES

End User Service Desk

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Domain Management **Service Delivery Manager** **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	7 years of experience in the management of IM/IT service desks, teams, budgets and contracts in a Government or large corporate environment of 5,000 or more end users	
M2	7 years of experience producing and implementing comprehensive Monthly Action Plans ("MAP") for Service Desk optimization such as: • SD metrics • implementation of SD process improvements • training gaps • client service expectations	
M3	7 years of ' experience defining technical specification workload estimates in relation to SD services	
M4	7 years of experience ensuring that the Service Level Targets are met and that those missed are documented	
M5	7 years of experience in monitoring and testing contingency plans for critical Service Desk systems	
M6	7 years of 'experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf (COTS) office products such as MS Office. Technical support can include such as password resets, hardware issues related to damaged peripherals, software related issues such as non-responding applications, identification of security incidents	

	such as viruses and malware security incidents such as viruses and malware	
M7	7 years providing expertise and guidance with regards to a Service Desk environment for Service Desk functions related to workstations, server and client environments	
M8	7 years of experience implementing corrective actions in a call centre environment related to call, incident, problem and change management and escalation processes	
M9	7 years of experience reviewing service management status reports including data related to quality assurance, daily and weekly call statistics, issue/problem resolutions	
M10	7 years of experience in the analysis of IT Service Desk workload reporting to determine process improvements in areas such as call resolution, customer service	
M11	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
End User Service Desk		
Domain Management **Domain Team Lead** **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	5 years' experience providing Information Technology technical support services in client operating systems, networks operating software, or commercial-off the-shelf ("COTS") office products (MS Office). Technical support can include such as password resets, hardware issues related to damaged peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware	

M2	5 years' experience in the management of IT projects and teams	
M3	5 years' experience implementing Management Action Plans ("MAP") in a Service Desk environment such as: • SD metrics • implementation of SD process improvements • client service expectations	
M4	5 years providing expertise and guidance with regards to a Service Desk environment for Service Desk functions related to workstations, server and client environments	
M5	5 years' experience implementing corrective actions in a call centre environment related to call, incident, problem and change management and escalation processes	
M6	5 years' experience determining technical workload specifications in relation to the Service Desk environment	
M7	5 years' experience reviewing service management status reports including data such as quality assurance, daily and weekly call statistics, issue/problem resolutions	
M8	5 years' experience in the analysis of IT Service Desk workload reporting to determine process improvements in areas such as call resolution, customer service	
M9	5 years' experience in the provision of IT support client services within an IT environment for a Government or large corporate environment of 5,000 or more end users	
M10	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Reporting Analyst **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	4 years' experience producing reports for a Service Desk environment such as overall expertise, knowledge and performance levels for each specific area of expertise, such as Service Desk Agents ("SDA") for call, incident, problem, change, as well as Account Administrator ("AA"), Task Flow Controller ("TFC") and change requests	
M2	4 years' experience in the use of spreadsheets for tracking workload metrics on calls, incidents, problems and changes on a daily, weekly, monthly and quarterly basis	
M3	4 years' experience in tracking of metrics related to a Service Desk environment such as metrics and volumetric that demonstrate optimal performance of Problem resolution and request processing	
M4	4 years' experience producing documentation related to collection of metrics such as weekly activity statistics, call metrics, service management metrics, monthly resource requirements based on workload, SLA obligations	
M5	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Quality Analyst **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	4 years' experience in providing quality assurance in a Service Desk environment in preparing things like quarterly reports on findings, deficiencies, degradation, problems with existing processes, procedures, Service Desk Agents and recommended corrective measures and/or improvements	
M2	4 years' experience with an enterprise class IT Service Management record, prioritize, match against other tickets in the system , track, document, assign and close call/incident, problem and IMAC/change tickets	
M3	4 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required	
M4	4 years' experience in the analysis of quality assurance data related to a Service Desk environment such as the effectiveness and performance of all service desk tasks	
M5	4 years' experience in the use of spreadsheets for quarterly samples tickets (calls taken and problem number assigned) and reports detailing Service Desk Agent resolution rates of problems	
M6	4 years' experience in tracking of quarterly samples tickets (calls taken and problem number assigned) and reports on the Service Desk's quality of Service Requests	
M7	4 years' experience producing reports for a Service Desk environment such as on the integrity and day-to-day procedures of the SD indicating where the quality of work has degraded, maintained, or improved	
M8	4 years' experience producing documentation related to collection of metrics such as problem resolutions and request	

	processing	
M9	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Client Delivery Executive **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	10 years' experience in developing and monitoring of Service Desk action plans, policies, and guidelines	
M2	10 years' experience in the analysis and engineering of Information Technology processes to optimize operations	
M3	10 years' experience in analysis of Service Desk reports to ensure client service objectives are met such as overall satisfaction and service levels are being met and to address Service Desk delivery issues	
M4	10 years' experience in customer relationship management with government departments or large private sector organizations with over 5,000 resources	
M5	7 years' Project Management experiences and valid certification	
M6	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Incident Management - Senior Service Desk Agent **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	4 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close Service Request l/incident, problem and IMAC/change tickets	
M2	4 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf (COTS) office products Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware	
M3	4 years' experience working with an Automatic Call Distribution telephony system log in and out, set status, generate reports as required	
M4	4 years' experience providing coaching/mentoring to team members in an IT environment	
M5	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Team Leader – Incident Management **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	5 years' experience working with an enterprise class IT Service Management tool, record, prioritize, match against other tickets in the system , track, document, assign and close Service Request l/incident, problem and IMAC/change tickets	
M2	5 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products. Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware of security incidents such as viruses and malware	
M3	5 years' experience interacting with different levels of IT technical support groups such as to resolve support issues, participate in projects	
M4	5 years leading a team of professionals in the delivery of IT services such as: • call management • on-line support • problem and incident management • escalation	
M5	5 years' experience in the documentation of technical IT solutions	
M6	5 years' experience providing coaching to IT clients and team members	

M9	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Call Management - Intermediate Service Desk Agent **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	3 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf (COTS) office products. Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware	
M2	3 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close service request l/incident, problem and change tickets	
M3	3 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required	
M4	Valid Federal Government Level II Secret Security Level or Enhanced Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Call Management - Junior Service Desk Agent **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	2 year experience or an acceptable combination of education, training, and/or experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products Technical support can include password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware	
M2	2 year experience OR an acceptable combination of education, training, and/or experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close service Request l/incident, problem and/change tickets	
M3	2 year experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required	
M4	Valid Federal Government Level II Secret Security Level or Enhanced Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Senior Account Administrator **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	4 years' experience providing technical support in an IT environment	
M2	4 years' experience in providing account administration services in Microsoft Active Directory	
M3	4 years' experience working with an enterprise-class IT Service Management tool	
M4	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Intermediate Account Administrator **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	3 years' experience providing technical support in an IT environment	
M2	3 years' experience in providing account administration services in Microsoft Active Directory	
M3	3 years' experience working with an enterprise-class IT Service Management tool	
M4	Valid Federal Government Level II Secret Security Level or Enhanced Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Junior Service Order Agent **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	2 year experience OR an acceptable combination of education, training, and/or experience providing technical support in an IT environment	
M2	2 year OR an acceptable combination of education, training, and/or experience providing account administration services in Microsoft Active Directory	
M3	2 years' experience working with an enterprise-class IT Service Management tool	
M4	Valid Federal Government Level II Secret Security Level or Enhanced Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Flow Controller **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	3 years' experience providing technical support in an IT environment	
M2	3 years' experience working with an enterprise-class IT Service Management Tool	
M3	Valid Federal Government Level II Secret Security Level or Enhanced Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
End User Service Desk		
Team Lead **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	5 years' experience providing technical support in an IT environment	
M2	5 years' experience providing account administration services in Microsoft Active Directory	
M3	5 year experience working with an enterprise-class IT Service Management tool	
M4	5 years leading a team of professionals in the delivery of IT services	
M5	5 years' experience providing coaching to clients and team members	
M6	Valid Federal Government Level II Secret Security Level Clearance	

Enterprise Service Desk

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Service Desk		
Domain Management **Service Delivery Manager** **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	7 years of experience in the management of IM/IT service desks, teams, budgets and contracts in a Government or large corporate environment of 5,000 or more end users	
M2	7 years of experience producing and implementing comprehensive Monthly Action Plans ("MAP") for Service Desk optimization such as: • SD metrics • implementation of SD process improvements • training gaps • client service expectations	
M3	7 years of ' experience defining technical specification workload estimates in relation to SD services	
M4	7 years of experience ensuring that the Service Level Targets are met and that those missed are documented	
M5	7 years of experience in monitoring and testing contingency plans for critical Service Desk systems	
M6	7 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products such as MS Office. Technical support can include such as password resets, hardware issues, software related issues such as non-responding applications, identification of security incidents such as viruses and malware security	

	incidents such as viruses and malware as well as any other type of issues related to Infrastructure component.	
M7	7 years providing expertise and guidance with regards to a Service Desk environment for Service Desk functions related to workstations, server and client environments	
M8	7 years of experience implementing corrective actions in a call centre environment related to call, incident, problem and change management and escalation processes	
M9	7 years of experience reviewing service management status reports including data related to quality assurance, daily and weekly call statistics, issue/problem resolutions	
M10	7 years of experience in the analysis of IT Service Desk workload reporting to determine process improvements in areas such as call resolution, customer service	
M11	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Service Desk		
Domain Management **Domain Team Lead** **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	5 years' experience providing Information Technology technical support services in client operating systems, networks operating software I or commercial-off the-shelf ("COTS") office products (MS Office). Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware as well as any other type of issues related to Infrastructure component.	
M2	5 years' experience in the management of IT projects and teams	
M3	5 years' experience implementing Management Action Plans ("MAP") in a Service Desk environment such as: • SD metrics • implementation of SD process improvements • client service expectations	
M4	5 years providing expertise and guidance with regards to a Service Desk environment for Service Desk functions related to workstations, server and client environments	
M5	5 years' experience implementing corrective actions in a call centre environment related to call, incident, problem and change management and escalation processes	
M6	5 years' experience determining technical workload specifications in relation to the Service Desk environment	

M7	5 years' experience reviewing service management status reports including data such as quality assurance, daily and weekly call statistics, issue/problem resolutions	
M8	5 years' experience in the analysis of IT Service Desk workload reporting to determine process improvements in areas such as call resolution, customer service	
M9	5 years' experience in the provision of IT support client services within an IT environment for a Government or large corporate environment of 5,000 or more end users	
M10	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Service Desk		
Domain Reporting Analyst **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	4 years' experience producing reports for a Service Desk environment such as overall expertise, knowledge and performance levels for each specific area of expertise, such as Service Desk Agents ("SDA") for call, incident, problem, change, as well as Account Administrator ("AA"), Task Flow Controller ("TFC") and change requests	
M2	4 years' experience in the use of spreadsheets for tracking workload metrics on calls, incidents, problems and changes on a daily, weekly, monthly and quarterly basis	
M3	4 years' experience in tracking of metrics related to a Service Desk environment such as metrics and volumetric that demonstrate optimal performance of Problem resolution and request processing	

M4	4 years' experience producing documentation related to collection of metrics such as weekly activity statistics, call metrics, service management metrics, monthly resource requirements based on workload, SLA obligations	
M5	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Service Desk		
Domain Quality Analyst **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	4 years' experience in providing quality assurance in a Service Desk environment in preparing things like quarterly reports on findings, deficiencies, degradation, problems with existing processes, procedures, Service Desk Agents and recommended corrective measures and/or improvements	
M2	4 years' experience with an enterprise class IT Service Management record, prioritize, match against other tickets in the system , track, document, assign and close call/incident, problem and IMAC/change tickets	
M3	4 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required	
M4	4 years' experience in the analysis of quality assurance data related to a Service Desk environment such as the effectiveness and performance of all service desk tasks	
M5	4 years' experience in the use of spreadsheets for quarterly samples tickets (calls taken and problem number assigned) and reports detailing Service Desk	

	Agent resolution rates of problems	
M6	5 years' experience in tracking of quarterly samples tickets (calls taken and problem number assigned) and reports on the Service Desk's quality of Service Requests	
M7	4 years' experience producing reports for a Service Desk environment such as on the integrity and day-to-day procedures of the SD indicating where the quality of work has degraded, maintained, or improved	
M8	4 years' experience producing documentation related to collection of metrics such as problem resolutions and request processing	
M9	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Service Desk		
Client Delivery Executive **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	10 years' experience in developing and monitoring of Service Desk action plans, policies, and guidelines	
M2	10 years' experience in the analysis and engineering of Information Technology processes to optimize operations	
M3	10 years' experience in analysis of Service Desk reports to ensure client service objectives are met such as overall satisfaction and service levels are being met and to address Service Desk delivery issues	
M4	10 years' experience in customer relationship management with government departments or large	

	private sector organizations with over 5,000 resources	
M5	7 years' Project Management experience and valid certification	
M6	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Service Desk		
Incident Management - Senior Service Desk Agent **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	4 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close Service Request l/incident, problem and IMAC/change tickets	
M2	4 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware as well as any other type of issues related to Infrastructure component.	
M3	4 years' experience working with an Automatic Call Distribution telephony system log in and out, set status, generate reports as required	
M4	4 years' experience providing coaching/mentoring to team members in an IT environment	

M5	Valid Federal Government Level II Secret Security Level or Enhanced Level Clearance	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Service Desk		
Team Leader – Incident Management **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	5 years' experience working with an enterprise class IT Service Management tool, record, prioritize, match against other tickets in the system , track, document, assign and close Service Request l/incident, problem and IMAC/change tickets	
M2	5 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products. Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware of security incidents such as viruses and malware as well as any other type of issues related to Infrastructure component.	
M3	5 years' experience interacting with different levels of IT technical support groups such as to resolve support issues, participate in projects	
M4	5 years leading a team of professionals in the delivery of IT services such as: • call management • on-line support • problem and incident management	

	• escalation	
M5	5 years' experience in the documentation of technical IT solutions	
M6	5 years' experience providing coaching to IT clients and team members	
M9	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Service Desk		
Incident Management Escalation Coordinator **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	3 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close Service Request l/incident, problem and change tickets	
M2	3 years' experience in analysis and triage of IT service desk incidents	
M3	3 years' experience interacting with different levels of IT technical support groups to check active incident, problem and change tickets against service level targets and perform escalations and notifications to affected stakeholders	
M4	Valid Federal Government Level II Secret Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Service Desk		
Call Management - Intermediate Service Desk Agent **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	3 years' experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf (COTS) office products. Technical support can include such as password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware	
M2	3 years' experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close service request l/incident, problem and change tickets	
M3	3 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required	
M4	Valid Federal Government Level II Secret Security Level or Enhanced Security Level Clearance	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Service Desk		
Call Management - Junior Service Desk Agent **The Proposed Resource "must" demonstrate the following at a minimum**		
M1	2 year experience or an acceptable combination of education, training, and/or experience providing Information Technology technical support services in client operating systems, networks operating software or commercial-off the-shelf ("COTS") office products Technical support can include password resets, hardware issues related to damaged Peripherals, software related issues such as non-responding applications, identification of security incidents such as viruses and malware	
M2	2 year experience OR an acceptable combination of education, training, and/or experience working with an enterprise class IT Service Management tool to open, record, prioritize, match against other tickets in the system , track,, document, assign and close service Request l/incident, problem and/change tickets	
M3	2 years' experience working with an Automatic Call Distribution telephony system to log in and out, set status, generate reports as required	
M4	Valid Federal Government Level II Secret Security Level or Enhanced Security Level Clearance	

Enterprise Command Center and Data Center Operations

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
ECC Event Management Team Lead **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	4 years of experience as a supervisor or team lead in mid-range, mainframe or network operations	
M2	4 years' of experience in keeping operational resources current with client technical and operational requirements and procedures	
M3	4 years' of experience in using incident and change management processes including inputting or updating information into incident and change management systems	
M4	4 years' of experience in project control / coordination or project management	
M5	4 years' of experience working in a data centre environment	
M6	4 years' of experience working with Tivoli Enterprise Systems Management tool or equivalent enterprise ITSM tool	
M7	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 4 years' experience in a minimum of 12 of the following requirement		
Experience in using incident and change management processes including inputting or updating information into		
Incident and change management systems on 3 or more projects		

Experience in project coordination or project management on 3 or more projects	
Create, update, and implement operational procedures and/or checklists	
Monitor the performance of operations through the use of metrics	
Manage and/or coordinate incidents and/or change management as per ITIL guidelines	
Translate user requests into operational requirements	
Understanding and enforcing data centre Security procedures	
Monitor environmental systems and taking appropriate action	
Initiating / rebooting / troubleshooting Windows Server	
Initiating / rebooting / troubleshooting LINUX, UNIX	
Initiating / rebooting / troubleshooting OS390 or MVS/ESA	
System Automation tools (CA7)	
TELNET, SSH, REMOTE DESKTOP CONNECTION	
System security products (for example, SECURITY 3000, HITMAN, GUARDIAN)	
Tape Management System (MEDIA MANAGER or TMS or IBM/VTS)	
Create, update, and implement operational procedures and/or checklists on 3 or more projects	
Reading, understanding and identifying components of a network topology diagram	
Troubleshooting network related incidents	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
Production Support Analyst **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	4 years' experience administering operations	
M2	4 years' experience in coordinating and assisting with the incident and/or change management in an operational environment	
M3	4 years' experience in managing training and educational needs of the operations group	
M4	4 years' experience in project coordination	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 4 years' experience in a minimum of 15 of the following requirement		
Create, update, and implement operational procedures and/or checklists		
Monitor the performance of operations through the use of metrics		
Experience in using incident and change management processes including inputting or updating information into incident and change management systems on at least 3 projects		
Project management		
Experience working with Tivoli Enterprise Systems Management tool or equivalent		
Initiating / rebooting / troubleshooting OS390 or MVS/ESA		

Initiating / rebooting / troubleshooting Windows Server	
Initiating / rebooting / troubleshooting LINUX, UNIX	
Console Utilities & Diagnostic Tools (MVS/JES2, TSO/ISPF, IOF/SDSF)	
At least 2 of the following: CLISTS, JCL, SYSLOG, LOGREC, DUMPS	
System Management Tools (for example, WHATSUP PRO)	
System Automation (CA-7)	
At least 2 of the following: AF/OPERATOR, OPS/MVS, AUTOMATE X/C, AUTOMATION POINT, SA/390	
Security Systems (for example, TOP SECRET, RACF, AOF OPERATOR)	
Online Regions (CICS, DBS, IDMS, WEBService ProviderHERE)	
Monitoring (for example, OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)	
Tape Management System (MEDIA MANAGER or TMS or IBM/VTS)	
Reading, understanding and identifying components of a network topology diagram	
Troubleshooting network related incidents	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
ECC Event Management Senior Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	4 years' experience working in IT Operations in a data centre environment	
M2	4 years' experience in mainframe, server or network system monitoring	
M3	4 years' experience in batch processing	
M4	4 years' experience in using incident and Change management processes including inputting or updating information into event, incident and change management systems	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 4 years' experience in a minimum of 13 of the following requirement		
Operate mainframe, server computers, or networking infrastructures		
Experience in mainframe and server system monitoring on 4 or more projects or engagements		
Experience in using Event, incident and Change management processes including inputting or updating information into event, incident and change management systems on 4 or more projects		
Experience in mainframe batch processing on 4 or more projects		
Monitor data centre environmental systems		
Create, update, and implement operational procedures and/or checklists		

Experience in using system performance or diagnostic tools	
Initiating / rebooting / troubleshooting Windows Server	
Initiating / rebooting / troubleshooting LINUX, UNIX	
Initiating / rebooting / troubleshooting OS390 or MVS/ESA	
System Management Tools (for example, WHATSUP PRO)	
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)	
Online Regions (CICS, DB2, IDMS, WEBSPHERE)	
Batch Processing (CA-7, CONTROL-M, TWS)	
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)	
Communication tools (Telnet, or Remote Desktop Connection, or equivalent)	
Tape Management Systems (CONTROL-T or ZARA or RMM or TSM) or equivalent	
Reading, understanding and identifying components of a network topology diagram	
Troubleshooting network related incidents	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
ECC Event Management Intermediate Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	2 years' experience working in IT Operations in a data centre environment	
M2	2 years' experience in mainframe, server or network system monitoring	
M3	2 years' experience in batch processing	
M4	2 years' experience in using incident and Change management processes including inputting or updating information into event, incident and change management systems	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 2 years' experience in a minimum of 13 of the following requirement		
Operate mainframe or server computers		
Experience in mainframe and server system monitoring on 2 or more projects or engagements		
Experience in using Event, incident and Change management processes including inputting or updating information into event, incident and change management systems on 2 or more projects		
Experience in mainframe batch processing on 2 or more projects		
Monitor data centre environmental systems		
Create, update, and implement operational procedures and/or checklists		

Experience in using system performance or diagnostic tools	
Initiating / rebooting / troubleshooting Windows Server	
Initiating / rebooting / troubleshooting LINUX, UNIX	
Initiating / rebooting / troubleshooting OS390 or MVS/ESA	
System Management Tools (for example, WHATSUP PRO)	
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)	
Online Regions (CICS, DB2, IDMS, WEBSPHERE)	
Batch Processing (CA-7, CONTROL-M, TWS)	
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)	
Communication tools (Telnet, or Remote Desktop Connection, or equivalent)	
Tape Management Systems (CONTROL-T or ZARA or RMM or TSM) or equivalent	
Reading, understanding and identifying components of a network topology diagram	
Troubleshooting network related incidents	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
ECC Event Management Junior Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	1 years' experience working in IT Operations in a data centre environment	
M2	1 years' experience in mainframe, server or network system monitoring	
M3	1 years' experience in using incident and Change management processes including inputting or updating information into	
M4	1 years' experience and change management systems	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 1 years' experience in a minimum of 5 of the following requirement		
Operate mainframe or server computers on 2 or more client engagements		
Initiating / rebooting / troubleshooting Windows Server or LINUX or UNIX or OS390 or MVS/ESA		
System Management Tools (for example, WHATSUP PRO)		
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)		
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)		
Tape Management Systems (CONTROL-T or ZARA or RMM)		

Reading, understanding and identifying components of a network topology diagram	
Troubleshooting network related incidents	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
ITSM Senior Management Consultant **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	4 years' experience in operations management consulting	
M2	4 years' experience ITIL Intermediate Certificate in IT Service Management (ITIL v3, at least one ITIL Intermediate Module)	
M3	4 years' experience in planning IT Service Management (ITIL) implementations in a large data centre environment	
M4	4 years' experience in communicating plans and strategies to management and employees	
M5	4 years' experience in leading the implementation of IT Service Management (ITIL) projects	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 4 years' experience in a minimum of 6 of the following requirement		
Analysing operational statistics on at least 5 projects		
Working with service management tools (e.g. Infoman; Tivoli, etc.)		
Working with IT Service Management (ITIL) tools or systems in a data		

centre production environment on 3 or more projects	
Working as a Project Manager on at least 3 IT Service Management projects	
Developing procedures for IT Service Management (ITIL) on at least 3 projects	
Creating and updating data flow diagrams using Visio or equivalent flowcharting tool	
Providing training to IT personnel on 3 or more projects	
Experience in planning IT Service Management (ITIL) implementations in a large datacentre environment on at least 3 or more projects	
Experience in communicating plans and strategies to management and employees on at least 3 or more projects	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Command Center and Data Center Operations		
ITSM Intermediate Management Consultant **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	3 years' experience in operations management consulting	
M2	3 years' experience ITIL Intermediate Certificate in IT Service Management (ITIL v3, at least one ITIL Intermediate Module)	
M3	3 years' experience in planning IT Service Management (ITIL) implementations in a large data centre environment	
M4	3 years' experience in communicating plans and strategies to management and employees	

M5	3 years' experience in the implementation of IT Service Management (ITIL) projects	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 3 years' experience in a minimum of 7 of the following requirement		
Analysing operational statistics on at least 3 projects		
Working with service management tools (e.g. Infoman; Tivoli, etc.)		
Working with IT Service Management (ITIL) tools or systems in a data centre production environment		
Working as a team member on at least 3 IT Service Management (ITIL) projects		
Developing procedures for IT Service Management (ITIL) disciplines		
Creating and updating data flow diagrams using Visio or equivalent flowcharting tool		
Providing training to IT personnel		
Experience in planning IT Service Management (ITIL) implementations in a large data centre environment		
Experience in communicating plans and strategies to management and employees		
Creating and updating operational documentation		

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Command Center and Data Center Operations		
Operations Domain Manager **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		

M1	5 years' experience of management experience in IT service delivery in a data centre environment	
M2	5 years' experience analyzing and re-engineering existing business processes to optimize IT operations	
M3	5 years' experience in developing and monitoring high level plans, policies and guidelines	
M4	5 years' experience communicating IT operational plans and strategies with technical staff, nontechnical staff and senior management in written and oral presentation formats	
M5	5 years' experience managing an IT support team of at least 15 resources for a continuous period of at least 1 year	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 5 years' experience in a minimum of 7 of the following requirement		
Manage complex IT operations environments (multiple software and hardware platforms) on at least 2 projects		
Manage hardware, software and/or service integration		
IT project management on at least 3 projects		
Provide advice and guidance on the mapping of business to operational requirements		
Provide advice, guidance and document recommendations for modifying or implementing service delivery programs		
ITIL Foundation certification (v.2 or higher)		
IT service cost estimating related to IT operations service support and delivery		
Architecting or designing IT solutions		

Recommending and implementing process improvements or cost savings solutions in an IT operations environment	
Experience working with Treasury Board Enhanced Management Framework (EMF)	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
Project Control Office Analyst **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	4 years' experience of IT project control experience	
M2	4 years' experience Document management in an IT enterprise environment	
M3	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 4 years' experience in a minimum of 6 of the following requirement		
Create and update IT operational procedures, IT performance metrics and key indicator metrics for consistency, accuracy and completeness on 2 or more projects		
Using automated tools for statistical analysis		
Monitor Work results against plans through the use of metrics (key performance metrics, key performance indicators, quality metrics, workload metrics, and metrics reporting) on 2 or more projects		
Experience in using Event, incident and Change management processes including inputting or updating information into incident and change management systems on 2 or more projects		
Coordinate and/or update contractual documentation on 2 or more projects		
Produce monthly management and statistical reports		

ITIL Foundation certification (v.2 or higher)	
Implementing document management procedures on 2 or more projects	
Office Products (MS Word or Lotus WordPro and MS Excel or Lotus 123)	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Command Center and Data Center Operations		
ECC Senior Tape Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	3 years' experience working in IT Operations in a data center environment	
M2	3 years' experience in mainframe batch processing	
M3	3 years' experience in supervising IT resources	
M4	3 years' experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems	
M5	3 years' experience in mainframe and server system monitoring	
M6	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 3 year experience in a minimum of 16 of the following requirement		
Experience in mainframe batch processing on 2 or more projects or engagements		
Experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems on 3 or more projects		

Experience in mainframe and server system monitoring on 3 or more projects or engagements	
Operate mainframe or server computers on 2 or more client engagements	
Utilize system, performance and diagnostic tools (for example, OMEGAMON)	
Experience in mainframe batch processing on 2 or more projects	
Monitor data center environmental systems	
Create, update, and implement operational procedures and/or checklists	
Initiating / rebooting / troubleshooting Windows Server	
Initiating / rebooting / troubleshooting LINUX, UNIX	
Initiating / rebooting / troubleshooting OS390 or MVS/ESA	
Console Utilities & Diagnositc Tools (MVS/JES2, TSO/ISPF, IOF/SDSF)	
At least 2 of the following: CLISTS, JCL, SYSLOG, LOGREC, DUMPS	
System Management Tools (for example, WHATSUP PRO)	
System Automation (CA-7)	
At least 2 of the following: AF/OPERATOR, OPS/MVS, AUTOMATE X/C, AUTOMATION POINT, SA/390	
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)	
Online Regions (CICS, DB2, IDMS, WEBSPHERE)	
Batch Processing (CA-7, CONTROL-M, TWS)	
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)	
Tape Management Systems (CONTROL-T or ZARA or RMM)	

Reading, understanding and identifying components of a network topology diagram	
Troubleshooting network related Incidents	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Command Center and Data Center Operations		
ECC Intermediate Tape Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	2 years' experience working in IT Operations in a data center environment	
M2	2 years' experience in mainframe or server system monitoring	
M3	2 years' experience in batch processing	
M4	2 years' experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 2 year experience in a minimum of 13 of the following requirement		
Operate mainframe or server computers		
Experience in mainframe and server system monitoring on 2 or more projects or engagements		
Experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems on 2 or more projects		
Experience in mainframe batch processing on 2 or more projects		

Monitor data center environmental systems	
Create, update, and implement operational procedures and/or checklists	
Experience in using system performance or diagnostic tools	
Initiating / rebooting / troubleshooting Windows Server	
Initiating / rebooting / troubleshooting LINUX, UNIX	
Initiating / rebooting / troubleshooting OS390 or MVS/ESA	
System Management Tools (for example, WHATSUP PRO)	
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)	
Online Regions (CICS, DB2, IDMS, WEBSPHERE)	
Batch Processing (CA-7, CONTROL-M, TWS)	
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)	
Communication tools (Telnet, or Remote Desktop Connection, or equivalent)	
Tape Management Systems (CONTROL-T or ZARA or RMM or TSM) or equivalent	
Reading, understanding and identifying components of a network topology diagram	
Troubleshooting network related Incidents	

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Command Center and Data Center Operations		
ECC Junior Tape Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	1 year experience working in IT Operations in a data centre	

	environment	
M2	1 year experience in mainframe or server system monitoring	
M3	1 year experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems	
M4	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 1 year experience in a minimum of 5 of the following requirement		
Operate mainframe or server computers on 2 or more client engagements		
Initiating / rebooting / troubleshooting Windows Server or LINUX or UNIX or OS390 or MVS/ESA		
System Management Tools (for example, WHATSUP PRO)		
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)		
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)		
Tape Management Systems (CONTROL-T or ZARA or RMM)		
Reading, understanding and identifying components of a network topology diagram		
Troubleshooting network related Incidents		

Mandatory	**Qualifications**	**Requirement Met (Y/N)**
Enterprise Command Center and Data Center Operations		
ECC Tape Analyst **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	1 year tape library operations experience	
M2	1 year experience working with one of the following tape management systems on 2 or more projects: CONTROL-T or	

	ZARA or RMM or TSM	
M3	1 year experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems	
M4	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 1 year experience in a minimum of 8 of the following requirement		
Experience in keeping operational resources current with client technical and operational requirements and procedures related to tape library software and hardware		
Experience researching and documenting impacts of new software and hardware releases on existing technologies related to tape library		
Create, update, and implement operational procedures and/or checklists		
Experience conducting workload and capacity planning on data center tape library requirements		
Experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems on 2 or more projects		
Initiating / rebooting / troubleshooting OS390 or MVS/ESA		
Console Utilities & Diagnostic Tools (MVS/JES2 or TSO/ISPF or IOF/SDSF		
Experience working with CLISTS or JCL or SYSLOG or LOGREC or FATS/FATAR		
System Management Tools (for example, WHATSUP PRO)		
System Automation Tools (CONTROL-D or OPS/MVS)		
Experience working with AF/OPERATOR or AUTOMATE X/C or AUTOMATION POINT		

Experience working with ATLS or IBM/VTS or SMS or TMS	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
ECC Senior Facility Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	3 years' experience working in IT Operations in a data center environment	
M2	3 years' experience in mainframe batch processing	
M3	3 years' experience in supervising IT resources	
M4	3 years' experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems	
M5	3 years' experience in mainframe and server system monitoring	
M6	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 3 year experience in a minimum of 16 of the following requirement		
Experience in mainframe batch processing on 2 or more projects or engagements		
Experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems on 3 or more projects		
Experience in mainframe and server system monitoring on 3 or more projects or engagements		
Operate mainframe or server computers on 2 or more client		

engagements	
Utilize system, performance and diagnostic tools (for example, OMEGAMON)	
Experience in mainframe batch processing on 2 or more projects	
Monitor data center environmental systems	
Create, update, and implement operational procedures and/or checklists	
Initiating / rebooting / troubleshooting Windows Server	
Initiating / rebooting / troubleshooting LINUX, UNIX	
Initiating / rebooting / troubleshooting OS390 or MVS/ESA	
Console Utilities & Diagnositc Tools (MVS/JES2, TSO/ISPF, IOF/SDSF)	
At least 2 of the following: CLISTS, JCL, SYSLOG, LOGREC, DUMPS	
System Management Tools (for example, WHATSUP PRO)	
System Automation (CA-7)	
At least 2 of the following: AF/OPERATOR, OPS/MVS, AUTOMATE X/C, AUTOMATION POINT, SA/390	
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)	
Online Regions (CICS, DB2, IDMS, WEBSPHERE)	
Batch Processing (CA-7, CONTROL-M, TWS)	
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)	
Tape Management Systems (CONTROL-T or ZARA or RMM)	
Reading, understanding and identifying components of a network topology diagram	

Troubleshooting network related Incidents	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
ECC Intermediate Facility Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	2 years' experience working in IT Operations in a data center environment	
M2	2 years' experience in mainframe or server system monitoring	
M3	2 years' experience in batch processing	
M4	2 years' experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems	
M5	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 2 year experience in a minimum of 13 of the following requirement		
Operate mainframe or server computers		
Experience in mainframe and server system monitoring on 2 or more projects or engagements		
Experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems on 2 or more projects		
Experience in mainframe batch processing on 2 or more projects		
Monitor data center environmental systems		

Create, update, and implement operational procedures and/or checklists	
Experience in using system performance or diagnostic tools	
Initiating / rebooting / troubleshooting Windows Server	
Initiating / rebooting / troubleshooting LINUX, UNIX	
Initiating / rebooting / troubleshooting OS390 or MVS/ESA	
System Management Tools (for example, WHATSUP PRO)	
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)	
Online Regions (CICS, DB2, IDMS, WEBSPHERE)	
Batch Processing (CA-7, CONTROL-M, TWS)	
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)	
Communication tools (Telnet, or Remote Desktop Connection, or equivalent)	
Tape Management Systems (CONTROL-T or ZARA or RMM or TSM) or equivalent	
Reading, understanding and identifying components of a network topology diagram	
Troubleshooting network related Incidents	

Mandatory	Qualifications	Requirement Met (Y/N)
Enterprise Command Center and Data Center Operations		
ECC Junior Facility Operator **The Proposed Resource "must" demonstrate the following at a minimum within the last 8 years'**		
M1	1 year experience working in IT Operations in a data centre environment	
M2	1 year experience in mainframe or server system monitoring	
M3	1 year experience in using Incident and Change management processes including inputting or updating information into Incident and Change Management systems	
M4	Valid Federal Government Level II Secret Security Level Clearance	
The proposed resource must meet a minimum of 1 year experience in a minimum of 5 of the following requirement		
Operate mainframe or server computers on 2 or more client engagements		
Initiating / rebooting / troubleshooting Windows Server or LINUX or UNIX or OS390 or MVS/ESA		
System Management Tools (for example, WHATSUP PRO)		
Security Systems (for example, TOP SECRET or RACF or AOF OPERATOR)		
Monitoring (for example OMEGAMON, NETVIEW, BMC PATROL, CONCORDE)		
Tape Management Systems (CONTROL-T or ZARA or RMM)		
Reading, understanding and identifying components of a network topology diagram		
Troubleshooting network related Incidents		

APPENDIX F TO ANNEX A

CERTIFICATIONS AT THE TASK AUTHORIZATION STAGE

1. Education and Experience

The Contractor certifies that all the information provided in the resume(s) and supporting material submitted, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Contractor to be true and accurate. Furthermore, the Contractor warrants that the individual(s) proposed is capable of performing the Work described in the Contract. Canada reserves the right to verify any information provided in this regard, and untrue statements may result in the TA response being declared non-responsive or another action the Minister may consider appropriate.

_____ _____
Print name of authorized individual & sign above Date

2. Status of Personnel

If the Contractor has proposed any individual in fulfillment of this Contract who is not an employee of the Contractor, the Contractor hereby certifies that it has written permission from such person (or the employer of such person) to propose the services of such person in relation to the work performed in fulfillment of this Contract and to submit such person's resume to Canada. The Contractor must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Contractor.

_____ _____
Print name of authorized individual & sign above Date

3. Availability of Personnel

The Contractor certifies that, should it be authorized to provide the services under any TA resulting from this Contract, the resource(s) proposed in the TA response will be available to commence performance of the Work within a reasonable time from the date of acceptance of the Task Authorization, or within the time specified in the TA Form, and will remain available to perform the Work in relation to the fulfillment of the requirement.

_____ _____
Print name of authorized individual & sign above Date

4. Certification of Language

The Contractor certifies that the proposed resource(s) in response to this TA is/are fluent in English. The individual(s) proposed is/are able to communicate orally and in writing without any assistance and with minimal errors in English.

_____ _____
Print name of authorized individual & sign above Date

ANNEX B

BASIS OF PAYMENT

For the provision of Professional Services, as and when requested by Canada through a validly issued Task Authorization, and in consideration of the Contractor satisfactorily completing all of it obligations in accordance with the Contract, the Contractor will be paid the following Firm All Inclusive Per Diem rates for work performed pursuant to this Contract, Applicable Taxes extra. The Firm All Inclusive Per Diem Rate will be pro-rated for partial days.

TRANSITION CHARGES	
Please detail the transition charges for the total assumption of the services. The Proposal will include all costs that will be or possibly be charged to SSC.	
Transition charges are a one-time cost	
Transition Charge Description	**One-Time Charges ($ CAD)**
Project Management	$ -
End User Service Desk - knowledge transfer	$ -
End User Service Desk - tools installation and setup	$ -
End User Service Desk - service setup (phone system, email integration etc.)	$ -
End User Service Desk - workstation setup	$ -
Request Fulfilment - knowledge transfer	$ -
Request Fulfilment - tools installation and setup	$ -
Request Fulfilment - service setup (phone system, email integration etc.)	$ -
Request Fulfilment - workstation setup	$ -
Enterprise Service Desk - knowledge transfer	$ -
Enterprise Service Desk - tools installation and setup	$ -
Enterprise Service Desk - service setup (phone system, email integration etc.)	$ -
Enterprise Service Desk - workstation setup	$ -
ECC - knowledge transfer	$ -
ECC- tools installation and setup	$ -
ECC - service setup (phone system, email integration etc.)	$ -
ECC - workstation setup	$ -
Data Centre Operations - knowledge transfer	$ -

Data Centre Operations - tools installation and setup	$ -
Data Centre Operations - service setup (phone system, email integration etc.)	$ -
Data Centre Operations - workstation setup	$ -
Invoice Testing	$ -
Total Transition Cost Services	

CATEGORY OF PERSONNEL

END USER SERVICE DESK			Fixed Per Diem Rate			
	CATEGORY OF PERSONNEL		Contract Period (3 years)	Option Period 1	Option Period 2	Option Period 3
001	EUSD	Service Delivery Manager				
002	EUSD	Domain Team Lead				
003	EUSD	Reporting Analyst				
004	EUSD	Quality Analyst				
005	EUSD	Client Delivery Executive				
006	EUSD	Senior Service Desk Agent				
007	EUSD	Team Lead				
008	EUSD	Intermediate Service Desk Agent				
009	EUSD	Junior Service Desk Agent				
010	EUSD	Senior Account Administrator				
011	EUSD	Intermediate Account Administrator				
012	EUSD	Junior Service Order Agent				
013	EUSD	Flow Controller				
014	EUSD	Team Lead				

ENTERPRISE SERVICE DESK			Fixed Per Diem Rate			
CATEGORY OF PERSONNEL			Contract Period (3 years)	Option Period 1	Option Period 2	Option Period 3
015	ESD	Domain Management Service Delivery Manager				
016	ESD	Domain Team Lead				
017	ESD	Domain Reporting Analyst				
018	ESD	Domain Quality Analyst				
019	ESD	Domain Client Delivery Executive				
020	ESD	Incident Management Senior SDA				
021	ESD	Incident Management Team Lead				
022	ESD	Incident Management Escalation Coordinator				
023	ESD	Intermediate Service Desk Agent				
024	ESD	Junior Service Desk Agent				

ENTERPRICE COMMAND CENTRE AND DATA CENTRE OPERATIONS			Fixed Per Diem Rate			
CATEGORY OF PERSONNEL			Contract Period (3 years)	Option Period 1	Option Period 2	Option Period 3
025	ECC	ECC Event Management Team Lead				
026	ECC	Production Support Analyst				
027	ECC	ECC Event Management Senior Operator				
028	ECC	ECC Event Management Intermediate Operator				
029	ECC	ECC Event Management Junior Operator				
030	ECC	ITSM Senior Management Consultant				
031	ECC	ITSM Intermediate Management Consultant				
032	ECC	Operations Domain Manager				
033	ECC	Project Control Office Analyst				
034	DCO	ECC Senior Tape Operator				
035	DCO	ECC Intermediate Tape Operator				
036	DCO	ECC Junior Tape Operator				

ENTERPRICE COMMAND CENTRE AND DATA CENTRE OPERATIONS			Fixed Per Diem Rate			
CATEGORY OF PERSONNEL			Contract Period (3 years)	Option Period 1	Option Period 2	Option Period 3
037	DCO	ECC Tape Analyst				
038	DCO	ECC Senior Facility Operator				
039	DCO	ECC Intermediate Facility Operator				
040	DCO	ECC Junior Facility Operator				

ANNEX C

SECURITY REQUIREMENTS CHECK LIST
(See attached PDF SRCL)

ANNEX D

FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY - CERTIFICATION

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with such request by Canada will also render the bid non-responsive or will constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit HRSDC-Labour's website.

Date: _____(YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the *Employment Equity Act.*

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 employees (combined work force includes: permanent full-time, permanent part-time and temporary employees [temporary employees only includes those who have worked 12 weeks or more during a calendar year and who are not full-time students]).

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1. The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with HRSDC-Labour.

OR

( ) A5.2. The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to HRSDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to HRSDC-Labour.

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions)

ANNEX E

INSURANCE REQUIREMENTS

1. The Contractor must obtain Commercial General Liability Insurance, and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature, but for not less than $2,000,000 per accident or occurrence and in the annual aggregate.

2. The Commercial General Liability policy must include the following:

   a. Additional Insured: Canada is added as an additional insured, but only with respect to liability arising out of the Contractor's performance of the Contract. The interest of Canada should read as follows: Canada, as represented by Public Works and Government Services Canada.
   b. Bodily Injury and Property Damage to third parties arising out of the operations of the Contractor.
   c. Products and Completed Operations: Coverage for bodily injury or property damage arising out of goods or products manufactured, sold, handled, or distributed by the Contractor and/or arising out of operations that have been completed by the Contractor.
   d. Personal Injury: While not limited to, the coverage must include Violation of Privacy, Libel and Slander, False Arrest, Detention or Imprisonment and Defamation of Character.
   e. Cross Liability/Separation of Insureds: Without increasing the limit of liability, the policy must protect all insured parties to the full extent of coverage provided. Further, the policy must apply to each Insured in the same manner and to the same extent as if a separate policy had been issued to each.
   f. Blanket Contractual Liability: The policy must, on a blanket basis or by specific reference to the Contract, extend to assumed liabilities with respect to contractual provisions.
   g. Employees and, if applicable, Volunteers must be included as Additional Insured.
   h. Employers' Liability (or confirmation that all employees are covered by Worker's compensation (WSIB) or similar program)
   i. Broad Form Property Damage including Completed Operations: Expands the Property Damage coverage to include certain losses that would otherwise be excluded by the standard care, custody or control exclusion found in a standard policy.
   j. Notice of Cancellation: The Insurer will endeavour to provide the Contracting Authority thirty (30) days written notice of policy cancellation.
   k. If the policy is written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Contract.
   l. Owners' or Contractors' Protective Liability: Covers the damages that the Contractor becomes legally obligated to pay arising out of the operations of a subcontractor.
   m. Non-Owned Automobile Liability - Coverage for suits against the Contractor resulting from the use of hired or non-owned vehicles.
   n. Litigation Rights: Pursuant to subsection 5(d) of the *Department of Justice Act*, S.C. 1993, c. J-2, s.1, if a suit is instituted for or against Canada which the Insurer would, but for this clause, have the right to pursue or defend on behalf of Canada as an Additional Named Insured under the insurance policy, the Insurer must promptly contact the Attorney General of Canada to agree on the legal strategies by sending a letter, by registered mail or by courier, with an acknowledgement of receipt.

      For the province of Quebec, send to:

      Director Business Law Directorate,
      Quebec Regional Office (Ottawa),
      Department of Justice,
      284 Wellington Street, Room SAT-6042,
      Ottawa, Ontario, K1A 0H8

      For other provinces and territories, send to:

Senior General Counsel,
Civil Litigation Section,
Department of Justice
234 Wellington Street, East Tower
Ottawa, Ontario K1A 0H8

A copy of the letter must be sent to the Contracting Authority. Canada reserves the right to co-defend any action brought against Canada. All expenses incurred by Canada to co-defend such actions will be at Canada's expense. If Canada decides to co-defend any action brought against it, and Canada does not agree to a proposed settlement agreed to by the Contractor's insurer and the plaintiff(s) that would result in the settlement or dismissal of the action against Canada, then Canada will be responsible to the Contractor's insurer for any difference between the proposed settlement amount and the amount finally awarded or paid to the plaintiffs (inclusive of costs and interest) on behalf of Canada.

ATTACHMENT 3.1 – PRICING TABLES

Bidders are required to complete the following pricing tables.

See attached 3.1 Excel Pricing Tables

ATTACHMENT 4.1 – TECHNICAL CRITERIA

1.1 Technical Evaluation

1. 1.1.1a Mandatory Technical Criteria - CORPORATE

The Bidder must comply with the Mandatory Requirements specified below.

This list of qualifications is essential and must be met by the contractor to perform the required tasks and produce deliverables outlined in the Statement of Work. The information provided about the proposed contractor must clearly describe how each of the qualifications in the list is met. Failure to adequately describe how a qualification is met will be determined as "not met". If requested, the contractor must provide examples and reference information (may be checked) of their experience in the following:

To facilitate bid preparation and evaluation, Bidders must prepare and submit their proposal using the tables provided. When completing the grids, the specific information which demonstrates the requested criteria and reference to the page number of the bid should be incorporated so that the evaluator can verify this information.

Bidder Capability- Mandatory		Evaluation Criteria	Location in Proposal
Corporate Capability and Experience			
M1	Customer Reference: The Bidder must identify two references to substantiate the information in Form 2– Client Reference Verification The reference must relate to providing IT Support Services, as described in the Annex A – Statement of Work. Each Contract Reference must detail the following a. Contract value must be $35,000,000CDN or more (Applicable taxes excluded); b. Contract was awarded anytime within the period of **August 1, 2007** and **August 1 , 2017**; and **c.** Contract duration was at a minimum of two consecutive years For each customer reference, The proposal must include a customer contact name, telephone number and email address, as well as a description of the referenced project, number of resources, type of services provided, total contract value. The Reference must be the individual with the management and financial responsibility for the referenced Contract		

M2	The Services and the position within the referenced contract must be similarly defined. More specifically, it must have included a minimum of 40 or more concurrent managed resources Information management/Information technology resources in a similar IT project to those required in Annex A – Statement of Work. Each referenced contract must indicate that the bidder performed at least 4 out of the 7 functions: 1) Service Delivery Manager; 2) Service Desk Agent Support; 3) Reporting Analyst; 4) Quality Analyst; 5) Enterprise Command Event Management Senior Operator; 6) Incident Management Team Lead; 7) ECC Event Team Lead 8) ITSM Senior Management Consultant		
Transition -In			
M3	The Bidder will be required to plan, manage and execute an effective transition-in of services from the incumbents to resources provided by the Bidder. The Bidder must provide a draft "Transition Plan" The response needs to include but not limited to: • Description of methodologies you will use to support your transition approach • A summary of key phases and/or activities required to accomplish the transition timeline and milestones using your above-described methodologies. • Indicate the specific benefits that will result from the full implementation of the transition plan. Benefits can be direct or indirect, short-term or long-term. Quantified benefits will be considered most relevant. • Identify transition risks and risk mitigation approaches in detail. The risk mitigation approaches are reasonable and can be practically employed at Shared Services Canada technical and organizational environment.		
Facility Clearance			

M4	The bidder must hold a valid Secret security facility clearance at the time of the bid submission. • Name of bidder as it appears on security clearance application form • Level of security clearance obtained • file number		

1.1.2 Point Rated Technical Criteria - Corporate

In this section, details should be provided regarding the qualifications, relevant experience and expertise. The experience of each bidder must be clearly identified by providing a summary/description of the previous projects worked on and indicating when the work was carried out, and the client. A minimum of 70% must be achieved to be considered compliant.

Corporate Technical Point-Rated Evaluation Criteria

Bidder Capability – Rated Evaluation Criteria		Evaluation Criteria	Max Points Achieved	Location in Proposal
Corporate Capability and Experience				
Transition -in				
R1	The bid should contain a description of a similar transition effort the Bidder was responsible for conducting the transitioned IN of services similar to Appendix “A” statement of work The description should include: R.1.1 – The transition occurred according to the transition plan R.1.2 – The transition occurred without disruption to client service attributable to the Bidders’s performance. R.1.3 – The transition occurred on time as per transition schedule R.1.4 – The transition occurred on budget The Proposal must contain a client reference and contact information in order to validate the Bidder’s assertions. It is acceptable that this reference by the same as the reference give in the Mandatory Corporate	5 points awarded per reference for each transition that occurred according to the transition plan 0 Points Awarded for Negative Assertions and Invalidated Positive Assertions No partial points 5 points awarded per reference = the transition occurred without disruption to the client service attributable to the bidder’s performance 0 Points Awarded for Negative Assertions and Invalidated Positive Assertions No partial points 5 points awarded per reference = the transition occurred on time as per transition schedule 0 Points Awarded for Negative Assertions and	40	

	Evaluation Annex X document if applicable.	Invalidated Positive Assertions 5 points awarded per reference = the transition occurred on budget 0 Points Awarded for not on budget		
Risk Management – SSC has identified 2 major risks. The bid shall address each of the identified risks below:				
Risk 1) Ability to recruit and retain adequately qualified personnel. The bid will be rated on the extent to which each of the following is clearly and comprehensively addressed.				
R2	The bid should contain a description of understanding of the risk described in Risk 1 – above	1 Point – Demonstrated understanding of the unique resource needs 1 point – demonstrated understanding of the challenges presented by the labour market for skilled resources	2	
R3	The potential impact to Canada of the risk identified in Risk 1	1 Point – Demonstrated understanding of the nature of work and impact on resources 1 point – demonstrated understanding of the importance of Key resources	2	

R4	The likelihood that the risk identified in Risk 1 will materialize	1 Point – Demonstrated understanding of historical experience with typical turnover of resources. 1 point – demonstrated understanding of the probability that this risk will materialize in this Contract	2	
R5	The bidder's risk mitigation plan for the risk identified in Risk 1	2 Point – Demonstrated mitigation of risks. 2 Points - Demonstrated contingent actions for risks identified if mitigation steps fail	4	
R6	The Bidder's plans to monitor and control the risk identified in Risk 1 throughout the contract	1 Point – Demonstrated mechanism to monitor the risk throughout the contract 1 Point – Demonstrate process to keep contract authority/technical authority informed on status of this risk	2	
Risk 2) Ability to provide timely and effective training for personnel with to ensure resource forecast staffing levels are met. The bid will be rated on the extent to which each of the following is clearly and comprehensively addressed.				
R7	The bid should contain a description of understanding of the risk described in Risk 2 – above	1 Point – Demonstrated understanding of the unique skills and knowledge requirements 1 point – demonstrated understanding of the required balance between on the job training and formal training programs	2	

R8	The potential impact to Canada of the risk identified in Risk 2	1 Point – Demonstrated understanding of the nature of work and impact on resource skills and knowledge requirements 1 point – demonstrated understanding of the importance of Key sets	2	
R9	The likelihood that the risk identified in Risk will materialize	1 Point – Demonstrated understanding of historical experience with training issues in this work environment 1 point – demonstrated understanding of the probability that this risk will materialize in this Contract	2	
R10	The bidder's risk mitigation plan for the risk identified in Risk 2	2 Point – Demonstrated mitigation of risks identified in Risk 2 2 Points - Demonstrated contingent actions for risks identified in Risk 2 if mitigation steps fail	4	
R11	The Bidder's plans to monitor and control the risk identified in Risk 2 throughout the contract	1 Point – Demonstrated mechanism to monitor the risk throughout the contract 1 Point – Demonstrate process to keep contract authority/technical authority informed on status of this risk	2	
Total Maximum Points Achievable			64	
Minimum Points – 70%			45	

FORM 1

BID SUBMISSION FORM

BID SUBMISSION FORM		
Bidder's full legal name **[*Note to Bidders: Bidders who are part of a corporate group should take care to identify the correct corporation as the Bidder*.]**		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
Bidder's Procurement Business Number (PBN) [*see the Standard Instructions 2003*] **[*Note to Bidders: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder*.]**		
Jurisdiction of Contract: Province in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
Former Public Servants See the Article in Part 2 of the bid solicitation entitled Former Public Servant for a definition of "Former Public Servant".	Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	
	Is the Bidder a FPS who received a lump sum payment under the terms of a work force adjustment directive? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	
Number of FTEs [Bidders are requested to indicate, the total number of full-time-equivalent positions that would be created and maintained by the Bidder if it were awarded the Contract. This information is for information purposes only and will not be evaluated.]		
Security Clearance Level of Bidder *[include both the level and the date it was granted]* ***[Note to Bidders: Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security***		

clearance is not valid for the Bidder.]	
On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that: 1. The Bidder considers itself and its products able to meet all the mandatory requirements described in the bid solicitation; 2. This bid is valid for the period requested in the bid solicitation; 3. All the information provided in the bid is complete, true and accurate; and 4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.	
Signature of Authorized Representative of Bidder	

FORM 2

CLIENT REFERENCE VERIFICATION FORM
FOR MANDATORY TECHNICAL CRITERIA

Bidder	Name:
	Address:

As a Reference for the firm identified above, by signing below, I confirm that I am a representative of the Organization identified below and that I have read and understood the Mandatory Technical Criteria described in the bid solicitation.

An email attestation from the primary or backup contact will be accepted. The email attestation must accompany the completed form(s) as an attachment and should include a statement in the email itself similar to the following: “As a Reference for the firm identified in the attached, by providing this email, I confirm that I am a representative of the Organization identified in the attached and that I have read and understood the Mandatory Technical Criteria described in the attached page(s)."

The Contact should enter "Yes" or "No" or "UR", where "UR" means Unable to Respond, for each Mandatory Technical Criterion (M.1 to M.2) in the table below. If the Contact does not enter "Yes" or "No" or "UR" for a Mandatory Technical Criterion, the response will deemed to be "No" for that Mandatory Technical Criterion.

By responding "Yes" in the table below to a Mandatory Technical Criterion, the Contact agrees that the Bidder named above has delivered all of the services in the quantities and/or durations specified for the Mandatory Technical Criterion under the contract referenced below.

By responding "No" in the table below to a Mandatory Technical Criterion, the Contact agrees that the Bidder named above has not delivered all of the services in the quantities and/or durations specified for the Mandatory Technical Criterion under the contract referenced below.

By responding “Unable to Respond” (“UR”) in the table below to a Mandatory Technical Criterion, the Contact agrees that it is unwilling or unable to provide any information about whether the Bidder named above has delivered all of the services in the quantities and/or durations specified for the Mandatory Technical Criterion under the contract referenced below. So that Canada can ensure this process is fair to all the Bidders, if the Contact chooses a response that indicates "Unable to Respond" for any of the Mandatory Technical Criteria in the table below, it will be treated as a "No" response.

Mandatory Technical Criteria:
(Client reference to complete)

Mandatory	*Requirement*	*Met*
M1 (a)	Contract value must be $35,000,000CDN or more (Applicable taxes excluded);	
M1(b)	Contract was awarded anytime within the period of August 1, 2007 and August 1 , 2017;	
M1(c)	Contract duration was at a minimum of two consecutive years	

M2	The Services and the position within the referenced contract must be similarly defined. More specifically, it must have included a minimum of 40 or more concurrent managed resources Information management/Information technology resources in a similar IT project to those required in Appendix A – Statement of Work. Each referenced contract must indicate that the bidder performed at least 4 out of the 7 functions: 1) Service Delivery Manager; 2) Service Desk Agent Support; 3) Reporting Analyst; 4) Quality Analyst; 5) Enterprise Command Event Management Senior Operator; 6) Incident Management Team Lead; 7) ECC Event Team Lead 8) ITSM Senior Management Consultant	

(Bidder to complete):

Client Organization Name: _____

Client Contract Number for Reference Project (if applicable): _____

Name of Project Authority / Executive:	
Project Name:	
Project Start and End Dates:	
Brief Project Description: (maximum of 250 words)	
Relevance to Evaluation Criteria: (maximum of 250 words)	

(Client reference to complete):

Primary Contact Information	Name: Title: Phone: Email: Signature: Date:
Backup Contact Information from the same organization	Name: Title: Phone: Email: Signature: Date:

FORM 3

CLIENT REFERENCE VERIFICATION FORM
FOR POINT RATED TECHNICAL CRITERIA

Bidder	Name:
	Address:

As a Reference for the firm identified above, by signing below, I confirm that I am a representative of the Organization identified below and that I have read and understood the Point Rated Technical Criteria described in the bid solicitation.

An email attestation from the primary or backup contact will be accepted. The email attestation must accompany the completed form(s) as an attachment and should include a statement in the email itself similar to the following: “As a Reference for the firm identified in the attached, by providing this email, I confirm that I am a representative of the Organization identified in the attached and that I have read and understood the Point Rated Technical Criteria described in the attached page(s)."

The Contact should enter "Yes" or "No" or "UR", where "UR" means Unable to Respond, for each Point Rated Technical Criterion (R.1)in the table below. If the Contact does not enter "Yes" or "No" or "UR" for a Point Rated Technical Criterion, the response will deemed to be "No" for that Point Rated Technical Criterion.

By responding "Yes" in the table below to a Point Rated Technical Criterion, the Contact agrees that the Bidder named above has delivered all of the services in the quantities and/or durations specified for the Point Rated Technical Criterion under the contract referenced below.

By responding "No" in the table below to a Point Rated Technical Criterion, the Contact agrees that the Bidder named above has not delivered all of the services in the quantities and/or durations specified for the Point Rated Technical Criterion under the contract referenced below.

By responding “Unable to Respond” (“UR”) in the table below to a Point Rated Technical Criterion, the Contact agrees that it is unwilling or unable to provide any information about whether the Bidder named above has delivered all of the services in the quantities and/or durations specified for the Point Rated Technical Criterion under the contract referenced below. So that Canada can ensure this process is fair to all the Bidders, if the Contact chooses a response that indicates "Unable to Respond" for any of the Point Rated Technical Criteria in the table below, it will be treated as a "No" response.

Point Rated Technical Criteria:
(Client reference to complete)

Rated	*Rated*	*Complete Yes/NO/UR*
R.1.1	The transition occurred according to the transition plan	
R.1.2	The transition occurred without disruption to client service attributable to the Bidders’s performance.	
R.1.3	The transition occurred on time as per transition schedule	
R.1.4	The transition occurred on budget	

(Bidder to complete):

Client Organization Name: _____

Client Contract Number for Reference Project (if applicable): _____

Name of Project Authority / Executive:	
Project Name:	
Project Start and End Dates:	
Brief Project Description: (maximum of 250 words)	
Relevance to Evaluation Criteria: (maximum of 250 words)	

(Client reference to complete):

Primary Contact Information	Name: Title: Role in the Project: Phone: Email: Signature: Date:
Backup Contact Information from the same organization	Name: Title: Role in the Project: Phone: Email: Signature: Date:

FORM 4

SUBSTANTIATION OF TECHNICAL COMPLIANCE FORM

Mandatory Technical Criteria that requires substantiation by the Bidder	Bidder Substantiation	Reference to additional Substantiating Materials included in Bid
M-1		
M-2		
M-3		
M.4		
Point-Rated Technical Criteria that requires substantiation by the Bidder	**Bidder Substantiation**	**Reference to additional Substantiating Materials included in Bid**
R-1		
R-2		
R-3		
R-4		
R-5		
R-6		
R-7		
R-8		
R-9		
R-10		
R-11		

FORM 5

CODE OF CONDUCT CERTIFICATION FORM

Adresse de courriel /E-mail Address:
Ministère/Department:
Dénomination sociale complète du fournisseur / Complete Legal Name of Supplier
Adresse du fournisseur / Supplier Address
NEA du fournisseur / Supplier PBN
Numéro de la demande de proposition **Request for Propsal Number**
Membres du conseil d'administration (Utilisez le format - Prénom Nom) **Board of Directors (Use format - first name last name)**
1. Membre / Director
2. Membre / Director
3. Membre / Director
Autres Membres/ Additional Directors: