RETURN RESPONSES TO:

RETOURNER LES RÉPONSES À:

C/O Mark Hall
Bid Receiving Shared Services Canada | Services partagés Canada
700 Montreal Road
Ottawa, Ontario
K1A 0P7

REQUEST FOR RESPONSES FOR EVALUATION

DEMANDE DE RÉPONSES POUR L'ÉVALUATION

Comments - Commentaires
This document contains a Security Requirement

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

Title – Sujet Internet Interconnection Services - les Services d'interconnexion Internet	
Solicitation No. – N° de l'invitation 10026415/A	**Date**
Client Reference No. – N° référence du client : 12-0737	
GETS Reference No. – N° de reference de SEAG	
File No. – N° de dossier C71.10026415/A.EF	**CCC No. / N° CCC - FMS No. / N° VME**

Solicitation Closes – L'invitation prend fin **at – à** 02 :00 PM **on – le** May 17, 2013	**Time Zone / Fuseau horaire** Eastern Standard Time (EST) / Heure Normale de l'Est (HNE)
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐	
Address Inquiries to : - Adresser toutes questions à: Mark Hall	**Buyer Id – Id de l'acheteur** C71
Telephone No. – N° de téléphone : 819-956-0251	**Email - Courriel** mark.hall@ssc-spc.gc.ca
Destination – of Goods, Services, and Construction: **Destination – des biens, services et construction :** See Herein Voir aux présentes	

Delivery required - Livraison exigée See Herein / Voir aux présentes	**Delivery Offered – Livraison proposée**

Issuing Office – Bureau de distribution
Shared Services Canada / Services partagés Canada
Procurement And Vendor Relationships
11 rue Laurier
Gatineau, Quebec
K1A 0S5

SHARED SERVICES CANADA

Internet Interconnection Services

REQUEST FOR RESPONSES FOR EVALUATION

RFRE no.: 10026415/A

REQUEST FOR RESPONSES FOR EVALUATION
INTERNET INTERCONNECTION SERVICES (IIS)
FOR
SHARED SERVICES CANADA (SSC)

TABLE OF CONTENTS

REQUEST FOR RESPONSES FOR EVALUATION
INTERNET INTERCONNECTION SERVICES (IIS)
FOR
SHARED SERVICES CANADA (SSC)

PART 1 GENERAL INFORMATION AND RESPONDENT INSTRUCTIONS

1.1 Introduction

1.1.1 This Request for Responses for Evaluation (RFRE) is being issued by Shared Services Canada.

1.1.2 The objective of this RFRE is to identify and select Successful Respondents to proceed to subsequent phases of this procurement process.

1.1.3 An overview of the entire procurement process can be found in Part 3 - Overview of Procurement Process.

1.1.4 Canada wishes to address, at the earliest stage, security functionality issues with commercial solutions proposed to address the Internet Interconnection Services (IIS) requirement. Accordingly, through this Request for Responses for Evaluation, Canada will pre-approve the list of Information Technology Products that is proposed to be part of the infrastructure or backbone that will interconnect with Canada's network in order to eliminate solutions representing a vulnerability or functionality threat to Canada. This is an issue of security and therefore evolving in nature and over time. The assessment of proposed solutions, however, will be applied uniformly based on the perceived threats at the time of closure of the RFRE.

1.2 Parts of the RFRE

Part 1 General Information & Respondent Instructions: provides an overview of the IIS requirements, and the instructions, clauses and conditions applicable to the RFRE.

Part 2 Response Preparation Instructions: provides Respondents with instructions on how to prepare their response to the RFRE.

Part 3 Overview of procurement Process: provides Respondents with an overview of the phases of the Procurement process.

Part 4 Evaluation Procedures and Selection of Successful Respondents: indicates how the evaluation of RFRE responses will be conducted, the evaluation criteria, and the basis of selecting the Respondents that will continue with the IIS procurement process following the Qualification Phase.

Part 5 Certifications: includes the certifications to be provided as part of the RFRE response.

The following annexes are part of this RFRE:

Annex A: IIS RFRE Submission Form;
Annex B: Security Requirements Checklist (SRCL);
Annex C: IT Products List; and
Annex E: DRAFT RFP.

This RFRE is neither a request for proposal nor a solicitation of bids or tenders and is intended only to pre-qualify Respondents. No contract will result from this RFRE. Given that this RFRE may be cancelled by Canada, it may not result in any of the subsequent procurement processes described in this document. Because the RFRE is not a tender, Respondents are welcome to withdraw from the process at any time.

The resulting contract clauses including the statement of work, which describes the form of contract that may result from the subsequent Request for Proposal has been included to assist respondents in the development of their Response.

1.3 Overview of the IIS Requirement

The Government of Canada (hereinafter referred to as Canada or GC) has a requirement for a diverse Internet Interconnection Service (IIS) that will provide it with the ability to access Public Internet Services and also aid in the delivery of programs and services to Canadians.

The following services make up the IIS requirement which will be delivered on an as-and-when-requested basis:

- providing the Internet Interconnection Services (IIS);
- providing Anti-Distributed Denial of Service scrubbing service (DDoS);
- the relocation of circuits; and
- any deliverables required by the Contract.

The services will be delivered in the National Capital Region (NCR) and the Toronto Area (TOR), Canada, excluding any locations in areas subject to any of the Comprehensive Land Claims Agreements.
The requirement consists of three redundant IIS Service Interface Points (SIP) provided under two or three separate resulting Contracts, two SIPs in the NCR and one SIP in the Toronto Area; where each SIP must have the capacity and the reliability to be able to handle all the Internet traffic in the event of the failure of the others. The contract will require the provision of additional IIS SIPs within the same GC Datacenter or to other GC Datacenters within the NCR and Toronto Area on an as and when requested basis.

The resulting contracts will be used by SSC 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 two or three contracts, each for a period of 3 years, plus a 1 year irrevocable option allowing Canada to extend the term of the contract.

1.4 Standard Instructions, Clauses and Conditions Applicable to the RFRE

1.4.1 All instructions, clauses and conditions identified in the RFRE 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 (PWGSC).

1.4.2 All references to PWGSC contained within the Standard Instructions will be interpreted as a reference to SSC.

1.4.3 Respondents who submit a response agree to be bound by the instructions, clauses and conditions of the RFRE.

1.4.4 Standard Instructions - Goods or Services - Competitive Requirements 2003 (2012-11-19) are incorporated by reference into and form part of the RFRE, except that:

1.4.4.1 Wherever the term “bid solicitation” is used, substitute "Request for Responses for Evaluation";

1.4.4.2 Wherever the term "bid" is used, substitute "response";

1.4.4.3 Wherever the term "Bidder(s)" is used, substitute "Respondent(s)";

1.4.4.4 Where ever the term “Supplier(s)” is used, substitute “Respondent(s)”;

1.4.4.5 This RFRE relates only to the potential to qualify to submit a bid in response to a subsequent Request for Proposal for IIS;

1.4.4.6 Subsection 5 (4), which discusses a validity period, does not apply, given that this RFRE invites Respondents simply to qualify. Canada will assume that all Respondents who submit a response continue to wish to qualify unless they advise the Contracting Authority in writing that they wish to withdraw their response;

1.4.4 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.

1.4.5 The text under Subsection 4 of Section 01 – Code of Conduct and Certifications of 2003 referenced above is replaced by:

Respondents should provide, with their response or promptly thereafter, a complete list of names of all Individuals who are currently directors of the Respondent. If such a list has not been received by the time the evaluation of responses is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to provide such a list within the required time frame will render the response non-responsive.

Canada may, at any time, request that a Respondent provide properly completed and Signed Consent Form (Consent to a Criminal Record Verification form – PWGSC-TPSGC 229) for any or all individuals named in the aforementioned list within a specified delay. Failure to provide such Consent Forms within the delay will result in the response being declared non-responsive.

The text under Subsection 5 of Section 01 – code of Conduct and Certifications of 2003 referenced above is replaced by:

The Respondent must diligently maintain the list up-to-date by informing Canada in writing of any change occurring during the validity period of the Response, and must also provide Canada, when requested, with the corresponding Consent Forms. The Respondent will also be required to diligently maintain the list and when requested, provide Consent Forms during the period of any contract arising from this procurement process.

1.5 Submission of Response

1.5.1 Responses must be submitted only to the SSC Bid Receiving Unit by the date, time and place indicated on the cover page of the RFRE, despite any instructions in 2003.

1.5.2 Due to the nature of the RFRE, responses transmitted by facsimile or e-mail to SSC will not be accepted.

1.6 Enquiries During the RFRE Response Period

1.6.1 All enquiries regarding the RFRE and DRAFT RFP must be submitted in writing to the Contracting Authority no later than 10 calendar days before the RFRE closing date. Enquiries received after that time may not be answered.

1.6.2 Respondents should reference as accurately as possible the numbered item of the RFRE to which the enquiry relates. Care should be taken by Respondents to explain each question in sufficient detail in order to allow Canada to provide an accurate answer.

1.6.3 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 request that the Respondent edit the question, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all Respondents. Enquiries not submitted in a form that can be distributed to all Respondents may not be answered by Canada.

1.6.4 It is the intention of Canada to answer all questions and answers (Q&As) regarding the DRAFT Request for Proposal (RFP) attached as an annex to the RFRE, at the RFRE Phase. In order to ensure that Respondents have knowledge of the requirement before responding to this RFRE, the Contracting Authority will not answer questions about the Statement of Work (SOW) during the RFP Phase. Respondents should ask all questions regarding Canada’s SOW described in the DRAFT RFP during the RFRE Phase.

1.7 Improvement of Requirement During RFRE

If Respondents consider that the specifications or Statement of Work contained in the draft Request for Proposal (DRAFT RFP) could be improved technically or technologically, Respondents are invited to make suggestions, in writing, to the Contracting Authority named in the draft resulting contract clauses. Respondents 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 Respondent will be given consideration provided they are submitted to the Contracting Authority in accordance with the article entitled, “Enquiries During the RFRE Response Period”. Canada will have the right to accept or reject any or all suggestions.

1.8 Applicable Laws

1.8.1 The relations between the parties will be governed by the laws in force in the Province of Ontario.

1.8.2 A Respondent may, at its discretion, substitute the applicable laws of a Canadian province or territory of its choice without affecting the validity of its response, by inserting the name of the Canadian province or territory of its choice in the RFRE Submission Form included as Annex A. If no other province or territory is specified, the Respondent acknowledges that the laws of Ontario are acceptable to it.

1.9 Submission of Only One Bid from a Bidding Group:

1.9.1.1 The submission of more than one response from members of the same responding group is not permitted in response to this RFRE. If the members of a responding group participate in more than one response, Canada will set aside all the bids.

1.9.1.2 For the purposes of this article, "**responding group**" means all entities (whether those entities include one or more natural persons, corporations, partnerships, limited liability partnerships, etc.) that are related to one another. Regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law, entities are considered "**related**" for the purposes of this bid solicitation if:

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

1.9.1.2.2 they are "related persons" or "affiliated persons" according to the *Canada Income Tax Act*;

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

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

PART 2 RESPONSE PREPARATION INSTRUCTIONS

2.1 Response Preparation Instructions

2.1.1 **Copies of Response**: Canada requests that Respondents provide their response as follows:

2.1.1.1 Annex A: RFRE Submission Form (1 hard copy)

2.1.1.2 Annex C: IT Products List (1 hard copy) and 1 soft copy on CD or DVD

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

2.1.2 **Canada's Policy on Green Procurement**: In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process. See the Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, Respondents are encouraged to:

2.1.2.1 use paper containing fibre certified as originating from a sustainably-managed forest and/or containing a minimum of 30% recycled content; and

2.1.2.2 use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, and using staples or clips instead of cerlox, duotangs or binders.

2.2 Contents of Response

2.2.1 **A complete RFRE response consists of the following:**

2.2.1.1 **Completed Annex A: IIS RFRE Submission Form:** Respondents should include the information contained in the RFRE Submission Form (Annex A) with their responses. Annex A provides a common form in which Respondents can provide information required for evaluation, such as contact names, the Respondent's Procurement Business Number, the Respondent'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 the information requested is not provided with the RFRE response, upon request by the Contracting Authority the Respondent must submit the information.

2.2.1.2 **Completed Annex C IT Products List:** The Respondents must include a complete list of IT Products.

Note to Respondents: Respondents must use RFRE Annex C to provide the information required by 2.2.1.2 in their Response.

2.2.1.3 **Network Diagram**

2.2.1.3.1 The Respondents must include a network diagram that includes at a minimum:

2.2.1.3.1.1 physical and logical network topology, depicting the nodes and connections amongst nodes in the network; and

2.2.1.3.1.2 details of the nodes in the network, protocols, bandwidths, etc.

2.2.1.4 **Certifications**

2.2.1.4.1 Respondents must submit the certifications required under RFRE Part 5.

2.3 Security Requirements

2.3.1 The contractor must, at all times during the performance of the Contract, Standing Offer or Supply Arrangement maintain a valid Designated Organization Screening (DOS) WITH Information Technology Security issued by Public Works and Government Services Canada – Industrial Security Program.

The contractor and/or its employees must EACH maintain a valid Reliability Status issued by Public Works and Government Services Canada – Industrial Security Program.

The contractor must maintain a valid Document Safeguarding Capability (DSC) at the Protected A level issued by Public Works and Government Services Canada – Industrial Security Program.

The contractor and/or its employees MUST NOT remove any Protected B, C 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 B, C 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) Justice Canada – Security of Information Act (Latest Edition);
b) Industrial Security Manual (Latest Edition).

2.4 Pricing

2.4.1 Pricing information for the IIS requirement is not to be included in the response to this RFRE.

Note to Respondents: *The Response provided by the successful Respondent may be incorporated into any resulting contract by reference, and may be included in the Priority of Documents clause in any resulting contract.*

PART 3 OVERVIEW OF THE PROCUREMENT PROCESS

3.1 Overview

3.1.1 The RFRE Phase is the first phase of the IIS multi-phase procurement process as summarized in Table 1. The RFRE defines the requirements for the RFP Phase. The objective of the RFRE Phase is to qualify Respondents (to be known as the "Successful Respondents") for further consideration in the IIS procurement process.

3.1.2 On July 12, 2012, Shared Services Canada invoked the National Security Exception under the trade agreements in respect of procurements related to email, networks and data centres. As a result, this requirement is subject to the National Security Exception.

3.1.3 Refer to Part 4 for a more detailed explanation of the RFRE Evaluation Procedures and Selection of Successful Respondents.

Table 1 - Summary of IIS Procurement Process

Procurement Phase	Objectives
RFRE	• Issue RFRE on the Government Electronic Tendering Service (MERX) • Obtain RFRE responses from Respondents • Evaluate RFRE responses • Select the Successful Respondents to continue to the DRAFT RFP phase
RFP	• Issue final RFP to all Successful Respondents • Obtain bid responses from the Bidders • Evaluate the bids
Contract Award	• Award the IIS contracts to the winning Bidders

PART 4 EVALUATION PROCEDURES AND SELECTION OF SUCCESSFUL RESPONDENTS

4.1 Evaluation Procedures

4.1.1 Responses will be assessed in accordance with the entire requirement of the RFRE.

4.1.2 The RFRE evaluation process is divided into the following 2 steps:

4.1.2.1 Step 1: Evaluation of IT Products List; and

4.1.2.2 Step 2: Selection of Qualified Suppliers.

4.2 Mandatory Technical Criteria

Each response will be reviewed to determine whether it meets the mandatory requirements of the RFRE. Any element of the RFRE identified with the words “must” or “mandatory” is a mandatory requirement. Responses that do not comply with each and every mandatory requirement will be disqualified.

4.2.1 **The Mandatory Technical Criteria are as follows:**

4.2.1.1 A completed IT product list in accordance with Annex C; and

4.2.1.2 A complete Network Diagram described as described in 2.2.1.3.

4.2.2 Canada will have the right to ask for additional information on any components listed in the Respondent’s IT Product List before issuance of the RFP. The Respondent will have 1 working day (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 response being disqualified.

4.2.3 The Contracting Authority will notify Respondents in writing whether their IT Products List is approved or rejected. If the Respondent’s IT Products List is approved, the Respondent will receive an approval letter along with a copy of the approved IT Products List.

4.2.4 If the Respondent’s IT Product List was not approved, the Respondent will have 10 calendar days following the receipt of Canada’s written notification to resubmit their IT Products List. If the Respondent’s IT Products List is rejected a second time, there will be no further opportunities to resubmit a new IT Products List and the Respondent will not be qualified to proceed to the next phase in the procurement process.

4.3 Step 2: Selection of Qualified Respondents

4.3.1 A response must comply with the requirements of the RFRE and meet all mandatory evaluation criteria to be declared a Qualified Supplier.

PART 5 CERTIFICATIONS

Compliance with the certifications Respondents provide to Canada is subject to verification by Canada during the response evaluation period, during the subsequent phases of the procurement process described in this RFRE, and after award of a contract. The Contracting Authority will have the right to ask for additional information to verify the Respondents' compliance with the certifications at any time before the award of a contract. The Respondent's Response will be disqualified and any bids submitted in subsequent phases will be declared non-responsive if any certification made by the Respondent 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 result in the response being disqualified.

The following Certifications are required with the Respondents Response which should be documented in Annex A - IIS RFRE Submission Form:

5.1 Federal Contractors Program - Certification

5.1.1 The Federal Contractors Program for Employment Equity (FCP) requires that some Respondents, including a Respondent who is a member of a joint venture, 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 Respondent is subject to the FCP, evidence of its commitment must be included with their response.

5.1.2 Respondents 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. Respondents 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.

5.1.3 If the Respondent does not fall within the exceptions enumerated in (5.1.4.1) or (5.1.4.2) below, or does not have a valid certificate number confirming its adherence to the FCP, the Respondent 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.

5.1.4 Each Respondent is requested to indicate in its bid whether it is:

5.1.4.1 not subject to FCP, having a workforce of fewer than 100 permanent full or part-time permanent employees, or temporary employees having worked 12 weeks or more in Canada;

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

5.1.4.3 subject to the requirements of FCP, because it has a workforce of 100 or more permanent full or part-time permanent employees, or temporary employees having worked 12 weeks or more in Canada, but it has not previously obtained a certificate number from HRSDC (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 Respondent; or

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

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

Note to Respondents: *Respondents are requested to use the IIS RFRE Submission Form (Annex A) to provide information about their status under this program. For a joint venture Respondent, this information must be provided for each member of the joint venture.*

5.2 Former Public Servant Certification

5.2.1 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, Respondents must provide the information required below.

5.2.2 For the purposes of this clause,

5.2.2.1 "**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:

5.2.2.1.1 an individual;

5.2.2.1.2 an individual who has incorporated;

5.2.2.1.3 a partnership made of former public servants; or

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

5.2.2.2 "**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.

5.2.2.3 "**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.

5.2.3 If the Respondent is an FPS in receipt of a pension as defined above, the Respondent must provide the following information with their response:

5.2.3.1 name of former public servant;

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

5.2.4 If the Respondent is an FPS who received a lump sum payment pursuant to the terms of a work force reduction program, the Respondent must provide the following information:

5.2.4.1 name of former public servant;

5.2.4.2 conditions of the lump sum payment incentive;

5.2.4.3 date of termination of employment;

5.2.4.4 amount of lump sum payment;

5.2.4.5 rate of pay on which lump sum payment is based;

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

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

5.2.5 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.

5.2.6 By submitting a response, the Respondent certifies that the information submitted by the Respondent in response to the above requirements is accurate and complete.

Note to Respondents: *Respondents are requested to provide the information required by this clause in their Bid Submission Form (Annex A).*

ANNEX A

IIS RFRE SUBMISSION FORM		
RFRE NO.: 10026415/A		
Respondent's full legal name **[*Note to Respondents: Respondents who are part of a corporate group should take care to identify the correct corporation as the Respondent*.]**		
Authorized Representative of Respondent for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
Respondent's Procurement Business Number (PBN) [*see the Standard Instructions 2003*] **[*Note to Respondents: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Respondent will be determined based on the legal name provided, not based on the PBN, and the Respondent will be required to submit the PBN that matches the legal name of the Respondent*.]**		
Jurisdiction of Contract: Province in Canada the Respondent wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
Canada's Official Language in which the Respondent will communicate with Canada during any subsequent process - indicate either English or French		
Former Public Servants See the Article in Part 5 of the RFRE entitled Former Public Servant Certification for a definition of "Former Public Servant".	Is the Respondent 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 5 entitled "Former Public Servant Certification"	

<table>
<tr><th colspan="3">IIS RFRE SUBMISSION FORM</th></tr>
<tr><td colspan="3">RFRE NO.: 10026415/A</td></tr>
<tr><td></td><td colspan="2">Is the Respondent a FPS who received a lump sum payment under the terms of a work force reduction program?
Yes ____ No ____
If yes, provide the information required by the Article in Part 5 entitled “Former Public Servant Certification”</td></tr>
<tr><td rowspan="4">Federal Contractors Program for Employment Equity (FCP EE) Certification:

If the Respondent is exempt, please indicate the basis for the exemption to the right. If the Respondent does not fall within the exceptions enumerated to the right, the Program requirements do apply and the Respondent is required either to:

(a) submit to the Department of HRSD form LAB 1168, Certificate of Commitment to Implement Employment Equity, DULY SIGNED; or
(b) submit a valid Certificate number confirming its adherence to the FCP-EE.

Respondents are requested to include their FCP EE Certification or signed LAB 1168 with their bid; if this information is not provided in the bid, it must be provided upon request by the Contracting Authority during evaluation.

For joint ventures, be sure to provide this information for each of the members of the joint venture.</td><td colspan="2">On behalf of the Respondent, by signing below, I also confirm that the Respondent [check the box that applies]:</td></tr>
<tr><td>(a) is not subject to Federal Contractors Program for Employment Equity (FCP-EE), because it has a workforce of less than 100 permanent full or part-time employees in Canada;</td><td></td></tr>
<tr><td>(b) is not subject to FCP-EE, because it is a regulated employer under the Employment Equity Act;</td><td></td></tr>
<tr><td>(c) is subject to the requirements of FCP-EE, because it has a workforce of 100 or more permanent full or part-time employees in Canada, but has not previously obtained a certificate number from the Department of Human Resources and Skills Development (HRSD) (having not bid on requirements of $200,000 or more), in which case a duly signed certificate of commitment is attached; OR

(d) is subject to FCP-EE, and has a valid certification number as follows: _____ (and has not been declared an Ineligible Contractor by HRSD).</td><td></td></tr>
<tr><td>Number of FTEs [Respondents are requested to indicate, the total number of full-time-equivalent positions that would be created and maintained by the Respondent if it were awarded the Contract. This information is for information purposes only and will not be evaluated.]</td><td colspan="2"></td></tr>
</table>

IIS RFRE SUBMISSION FORM	
RFRE NO.: 10026415/A	
Security Clearance Level of Respondent *[include both the level and the date it was granted]* ***[Note to Respondents: Please ensure that the security clearance matches the legal name of the Respondent. If it does not, the security clearance is not valid for the Respondent.]***	
As the **Authorized Representative of Respondent**, by signing below, I confirm that I have read and understood the entire RFRE including the documents incorporated by reference into the RFRE and the entire Response, and I certify that: 1. All the information provided in the RFRE Response is complete, true and accurate.	
Signature of Authorized Representative of Respondent	x.

Annex B - SRCL

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
10026415
Security Classification / Classification de sécurité Unclassified

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Shared Services Canada	2. Branch or Directorate / Direction générale ou Direction: Transformation and Services Strategy Design
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Internet Interconnect Services (IIS), to replace diverse and redudant Internet services under the expiring SCNet contracts.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

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

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
10026415
Security Classification / Classification de sécurité Unclassified

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

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

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

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

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

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

☑ RELIABILITY STATUS COTE DE FIABILITÉ	☐ CONFIDENTIAL CONFIDENTIEL	☐ SECRET SECRET	☐ TOP SECRET TRÈS SECRET
☐ TOP SECRET– SIGINT TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL NATO CONFIDENTIEL	☐ NATO SECRET NATO SECRET	☐ COSMIC TOP SECRET COSMIC TRÈS SECRET
☐ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

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

10. b) May unscreened personnel be used for portions of the work? — No / Non ☑ Yes / Oui ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — No / Non ☐ Yes / Oui ☐
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
10026415
Security Classification / Classification de sécurité
Unclassified

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

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

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

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

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

ANNEX D -DRAFT BID SOLICITATION
INTERNET INTERCONNECTION SERVICES
FOR
SHARED SERVICES CANADA

TABLE OF CONTENTS

List of Annexes to the Resulting Contract:

Annex A Statement of Work
Annex B IIS Pricing
Annex C Security Requirements Check List
Annex D Access to Crown Property for Telecommunications Services
Annex E Billing Format File

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

Attachment 4.1: Mandatory Technical Evaluation Criteria
Attachment 4.2: Price Evaluation Workbook

Forms: Form 1 - Bid Submission Form

BID SOLICITATION FOR

INTERNET INTERCONNECTION SERVICES FOR SHARED SERVICES CANADA

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;

Attachment 4.1 - Mandatory Technical Evaluation Criteria
Attachment 4.2 - Price Evaluation Workbook

Part 5 Certifications: includes the certifications to be provided;

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

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

Annex A - Statement of Work
Annex B - IIS Pricing
Annex C - Security Requirements Checklist (SRCL)
Annex D - Access to Crown Property for Telecommunications Services
Annex E - Billing Format File

1.2 Summary

Shared Services Canada (SSC) has a requirement for a diverse Internet Interconnection Service (IIS) that will provide it with the ability to access Public Internet Services and also aid in the delivery of programs and services to Canadians by Other Government Departments and Agencies.

The following services make up the IIS requirement which will be delivered on an as-and-when-requested basis:

- providing the Internet Interconnection Services (IIS);
- providing Anti-Distributed Denial of Service scrubbing service (DDoS);
- the relocation of circuits; and
- any deliverables required under the Contract.

The above services will be delivered in the National Capital Region (NCR) and Toronto Area (TOR), Canada, excluding any locations in areas subject to any of the Comprehensive Land Claims Agreements.

The Requirement consists of three redundant IIS Service Interface Points (SIP) provided by two or three separate Contractors, two in the NCR and one in the Toronto Area; where each SIP will have the capacity and the reliability to be able to handle all the Internet traffic in the event of the failure of the others.

The resulting contracts will be used by SSC 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 two or three contracts, each for a period of 3 years, plus a 1 one year irrevocable option allowing Canada to extend the term of the contract.

There is a security requirement associated with this requirement. For additional information, see Part 6 - Security, Financial and Other 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, Shared Services Canada 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.

1.3 Debriefings

After contract award, 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

2.1.1 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.

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

The 2003 (2012-11-19) 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.

The text under Subsection 4 of Section 01 – Code of Conduct and Certifications of 2003 referenced above is replaced by:

> Bidders should provide, with their bid or promptly thereafter, a complete list of names of all individuals who are currently directors of the Bidder. If such a list has 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 provide such a list within the required time frame will render the bid non-responsive. Bidders must always submit the list of directors before contract award.
>
> Canada may, at any time, request that a Bidder provide properly completed and Signed Consent Form (Consent to a Criminal Record Verification form – PWGSC-TPSGC 229) for any or all individuals named in the aforementioned list within a specified delay. Failure to provide such Consent Forms within the delay will result in the bid being declared non-responsive.

The text under Subsection 5 of Section 01 – code of Conduct and Certifications of 2003 referenced above is replaced by:

> The Bidder must diligently maintain the list up-to-date by informing Canada in writing of any change occurring during the validity period of the bid, and must also provide Canada, when requested, with the corresponding Consent Forms. The Bidder will also be required to diligently maintain the list and when requested, provide Consent Forms during the period of any contract arising from this bid solicitation.

2.1.3 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”

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

> Delete: sixty (60) days
>
> Insert: one-hundred twenty (120) days

2.1.5 The Standard Instructions – Goods and Services – Competitive Requirements 2003 is amended as follows: delete Section 08 Transmission by Facsimile, in its entirety.

2.1.6 The 2003-1 Supplemental Standard Instructions - Telecommunications (2008-05-12) are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003-1 and this document, this document prevails.

2.2 Submission of Bids

2.2.1 Bids must be submitted only to Shared Services Canada by the date, time and place indicated on page 1 of the bid solicitation.

2.2.2 Due to the nature of the bid solicitation, bids transmitted by facsimile to Shared Services Canada will not be accepted.

2.3 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.*

2.4 Enquires

2.4.1 All enquiries must be submitted in writing to the Contracting Authority no later than 10 calendar days before the bid closing date. Enquiries received after that time may not be answered.

2.4.2 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.

2.4.3 Canada will not be answering questions regarding the Statement of Work during the RFP Phase of the procurement process. This will be done at the RFRE Phase.

PART 3 BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

3.1.1 **Copies of Bid**: Canada requests that bidders provide their bid in separately bound sections as follows:

3.1.1.1 Section I: Technical Bid (1 final version and 3 hard copies) and 2 soft copies on CD or DVD

3.1.1.2 Section II: Financial Bid (1 final version) and 1 soft copy on CD or DVD

3.1.1.3 Section III: Certifications (1 hard copy final version)

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

3.1.1.5 If there is a discrepancy between the wordings in any of the copies, the final version will have priority over the wording in the copy.

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

3.1.2 **Format for Bid**: Canada requests that bidders follow the format instructions described below in the preparation of their bid:

3.1.2.1 use 8.5 x 11 inch (216 mm x 279 mm) paper;

3.1.2.2 use a numbering system that corresponds to the bid solicitation;

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

3.1.2.4 include a table of contents.

3.1.3 **Canada's Policy on Green Procurement**: In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process. See the Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, bidders are encouraged to:

3.1.3.1 use paper containing fibre certified as originating from a sustainably-managed forest and/or containing a minimum of 30% recycled content; and

3.1.3.2 use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, and using staples or clips instead of cerlox, duotangs or binders.

3.2 Section I: Technical Bid

3.2.1 In their technical bid, bidders must demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders must demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work. The technical bid must address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

3.2.2 The technical bid consists of the following:

3.2.2.1 **Bid Submission Form (Form 1)**: Bidders are requested to include the Bid Submission Form 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. 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.

3.2.2.2 **Attachment 4.1 - Mandatory Technical Evaluation Criteria:**

The technical bid must substantiate the compliance of the Bidder and its proposed solution with the specific criteria identified in Attachment 4.1, which is the requested format for providing the substantiation. The Mandatory Technical Evaluation Criteria attachment is not required to address any parts of this bid solicitation not referenced in the attachment. 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 Work. Simply stating that the Bidder or its proposed solution or product complies is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be declared non-responsive and disqualified. The substantiation should refer to additional documentation submitted with the bid - this information can be referenced in the "Reference" column of the attachment 4.1, where Bidders are requested to indicate where in the 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.

3.2.2.3 **IT Products Approval Letter**

The Bidder should include the Letter it received by Canada as a result of their response to RFRE no.: 10026415/A.

3.3 Section II: Financial Bid

3.3.1 **Pricing**: Bidders must submit their financial bid in accordance with Attachment 4.2 - Price Evaluation Workbook. The total amount of Goods and Services Tax, Quebec Sales Tax or Harmonized Sales Tax must be shown separately, if applicable. Unless otherwise indicated, bidders must include a single, firm, all-inclusive price quoted in Canadian dollars in each cell requiring an entry in the pricing tables.

3.3.2 **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 years. 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.

3.3.3 **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.

3.5 Exchange Rate Fluctuation

The requirement does not provide for exchange rate fluctuation protection. Any request for exchange rate fluctuation protection will not be considered and will render the bid non-responsive.

PART 4 EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

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

4.1.2 An evaluation team composed of representatives of SSC 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.

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

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

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

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

4.1.3.2.2 contact any or all references supplied by the Bidder to verify and validate any information submitted by the Bidder,

the Bidder must provide the information requested by Canada within 3 working days of a request by the Contracting Authority.

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

4.2 Technical Evaluation - Mandatory Technical Evaluation Criteria

4.2.1 Each bid will be reviewed to determine whether it meets the mandatory requirements of the bid solicitation. Any element of the bid solicitation identified with the words “must” or “mandatory” is a mandatory requirement. Bids that do not comply with each and every mandatory requirement will be declared non-responsive and be disqualified.

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

4.2.3 The mandatory requirements are described in Attachment 4.1 - Mandatory Technical Evaluation Criteria.

4.2.4 **Demonstration**

4.2.4.1 Canada may, but will have no obligation, to require that the top-ranked Bidder (identified after the financial evaluation) demonstrate any features, functionality and capabilities described in this bid solicitation or in its bid, in order to verify compliance with the requirements of this bid solicitation. If required, the demonstration must be conducted, at no cost to Canada, at a location in Canada agreed to by the Contracting Authority. Canada will provide no fewer than 10 working days of notice before the scheduled date for the demonstration. The demonstration must be conducted during normal business hours, to be determined by the Contracting Authority. Canada will pay its own travel and salary costs associated with any demonstration. Despite the written bid, if Canada determines during a demonstration that the

Bidder's proposed solution does not meet the mandatory requirements of this bid solicitation, the bid will be declared non-responsive.

4.3 Financial Evaluation

4.3.1 The financial evaluation will be conducted by calculating the Total Evaluated Bid Price for the NCR and the Total Evaluated Bid Price for the Toronto Area using the Pricing Tables in Attachment 4.2 completed by the bidders.

4.3.2 **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 a bidder.

4.4 Basis of Selection

4.4.1 A bid must comply with the requirements of the bid solicitation and meet all mandatory evaluation criteria to be declared responsive.

The two responsive bids with the lowest Total Evaluated Bid Price for the NCR will be recommended for contract award. In the event these two responsive bids do not have the lowest Total Evaluated Bid Price for the Toronto Area, then the responsive bid with the lowest Total Evaluated Bid Price for the Toronto Area will also be recommended for contract award.

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

.

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 in accordance with the articles below.

Compliance with the certifications bidders provide to Canada, this includes the certifications provided at the RFRE Phase, 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.

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.

5.1 Certifications Required by Supplemental Standard Instructions 2003-1

Bidders are required to submit the required regulatory certifications in accordance with Supplemental Standard Instructions - Telecommunications. Bidders should note that only tariffs to which the Bidder itself will be subject in performing the work are required to be submitted. It is the responsibility of the Bidder to manage its own relationship with any subcontractors who may be subject to tariffs.

5.2 Code of Conduct Certification

Bidders are required to submit a complete list of names of all individuals who are currently directors of the Bidder. If such a list has not been received by the time the evaluation of bids is completed, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Bidders must submit the list of directors before contract award, failure to provide such a list within the required time frame will render the bid non-responsive.

The Contracting Authority may, at any time during any resulting Contract Period, request that a Bidder provide properly completed and Signed Consent Forms (Consent to a Criminal Record Verification form – PWGSC-TPSGC 229) for any or all individuals named in the aforementioned list within a specified time period. Failure to provide such Consent Forms within the time period specified by the Contracting Authority will result in the bid being declared non-responsive.

PART 6 SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirement

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

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

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

6.1.3 In the case of a joint venture bidder, each member of the joint venture must meet the security requirements.

6.2 Financial Capability

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

6.2.2 In the case of a joint venture bidder, each member of the joint venture must meet the financial capability requirements.

PART 7 RESULTING CONTRACT CLAUSES

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

7.1 Requirement

7.1.1 _____ (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:

7.1.1.1 providing the Internet Interconnection Services (IIS), as and when requested;

7.1.1.2 providing Anti-Distributed Denial of Service scrubbing service (DDoS), as and when requested;

7.1.1.3 the relocation of circuits, as and when requested; and

7.1.1.4 any deliverables required by the Contract.

The services will be delivered in the National Capital Region (NCR) and the Toronto Area (TOR), both in Canada, excluding any locations in areas subject to any of the Comprehensive Land Claims Agreements.

7.1.2 **Client:** Under the Contract, the "**Client**" is Shared Services Canada ("SSC"), an organization with a mandate to provide shared services. This Contract will be used by SSC to provide shared services to its clients, which 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. SSC may choose to use this Contract for some or all of its clients and may use alternative means to provide the same or similar services.

7.1.3 **Reorganization of Client**: The Contractor's obligation to perform the Work will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of any Client. The reorganization, reconfiguration and restructuring of the Client includes the privatization of the Client, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Client. In connection with any form of reorganization, Canada may designate another department or government body as the Contracting Authority or Technical Authority, as required to reflect the new roles and responsibilities associated with the reorganization.

7.1.4 **Defined Terms**: Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Contract have the meanings given to them in the General Conditions or Supplemental General Conditions. Also, the following words and expressions have the following meanings:

7.1.4.1 "Federal Government Working Days (FGWDs)" means Monday to Friday excluding the following holidays as observed by Canada:

7.1.4.1.1 New Year's Day;

7.1.4.1.2 Good Friday and Easter Monday;

7.1.4.1.3 Victoria Day;

7.1.4.1.4 St-Jean Baptiste Day (June 24th);

7.1.4.1.5 Canada Day;

7.1.4.1.6 1st Monday in August;

7.1.4.1.7 Labour Day;

7.1.4.1.8 Thanksgiving Day;

7.1.4.1.9 Remembrance Day;

7.1.4.1.10 Christmas Day; and

7.1.4.1.11 Boxing Day.

7.2 Service Orders

7.2.1 Work which is to be provided under the Contract will be ordered by Canada by transmitting a Service Order (SO) to the Contractor.

7.2.2 The Work described in the SO must be in accordance with the scope of the Contract. The Contractor must not commence work until an authorized SO has been received by the Contractor. The Contractor acknowledges that any work performed before an authorized SO has been received will be done at the Contractor's own risk.

7.2.3 Whenever the Contractor receives a Service Order from the Contract Authority, the Contractor agrees to provide the Work, ordered, in accordance with the terms and conditions and at the prices/rates set out in the Contract. Regardless of when a Service Order is issued, all Service Orders automatically end no later than the last day of the Contract Period, and Canada is not required to cancel any Service Orders at the end of the Contract Period.

7.2.4 The Contractor must not charge Canada anything more than the total cost set out in the Service Order unless Canada has issued a Service Order Amendment authorizing the increased cost. 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.

7.2.5 The Contractor must, within 120 FGWDs of award of a Contract, develop a solution and implementation plan in consultation with Canada for the optimization of the electronic transfer of Service Order Requests through an approved Electronics Information Exchange Tool (EIET), Service Order Acceptance and Service Order Completion Notices in conjunction with Canada.

7.2.6 The Contractor agrees that Service Orders can be submitted by Canada for the ordering of Services 7 days per week, 24 hours per day, 365 days per year (7x24x365) through the approved EIET.

7.2.7 Once the EIET has been accepted by Canada, the Contractor must ensure that Service Orders and any Service Order Amendment received from Canada are accessible using the EIET.

7.2.8 A Service Order, at a minimum, will include the following information:

7.2.8.1 Service Order number;

7.2.8.2 Service Order period;

7.2.8.3 The Contract Number;

7.2.8.4 Description of the Work being ordered;

7.2.8.5 The specific work location(s), delivery location(s), and Service Delivery Points (SDPs);

7.2.8.6 The total estimated cost for the Work based on the rates and prices set out in the Contract as they apply to the Service Order period; and

7.2.8.7 The basis of payment and method of payment which apply to the Work being ordered.

7.3 Service Order Process

7.3.1 Canada will transmit a Service Order to the Contractor for Work that is to be provided under the Contract with a Requested Service Delivery Date.

7.3.2 The Contractor must provide a Service Order Acceptance (SOA), by email or approved communication method, within 1 Federal Government Working Day confirming receipt of the Service Order and update the Service Order status in the EIET to indicate it has been received.

7.3.3 Within 2 FGWDs that Contractor must provide Canada with a Committed Service Delivery Date (CSDD) which is subject to Canada's written approval. The CSDD is the date in which the Contractor is obligated to complete the Work in the SO.

7.3.4 If the Service Order cannot be completed by the CSDD, the Contractor must notify Canada, in writing as soon as possible prior to the CSDD, of the reason for the delay and provide a revised CSDD. This revised date is subject to written approval by Canada. If Canada does not approve the revised date, the original CSDD must remain unchanged.

7.3.5 Once Canada has approved the CSDD, the Work is applicable to the Service Delivery Interval (SDI) for that Service Order as shown in Table 4 below.

7.3.6 A Service Delivery Interval (SDI) is the amount of time that the Contractor is allowed to implement a Service Order. The starting point for the SDI is the date the CSDD was approved by Canada. The end point for the SDI is the approved CSDD. The Contractor must complete the delivery of the service according to Table 4 below.

7.3.7 The Contractor must notify Canada, by email, of the successful completion of the Contractor's standard acceptance tests by issuing, no later than 1 FGWD following the completion of the test, a Service Order Completion Notice (SOCN).

7.3.8 The SOCN must contain a formal statement by the Contractor that testing of the service has been fully completed and ready for use.

7.3.9 The SOCN must also stipulate the completion date of the Contractor's testing and include the test results.

7.3.10 The Service Delivery Intervals (SDIs) are shown in Table 4 – Service Delivery Interval requirements.

7.3.11 After receipt of the SOCN, Canada has the right to perform its own acceptance tests within ten FGWDs.

7.3.12 Where Canada has conducted an acceptance test within 10 FGWDs of the SOCN date and raised a trouble ticket within this period, the implementation of the Service Order is considered incomplete, and the Contractor cannot bill for the service.

7.3.13 The Contractor must immediately notify Canada by email of any trouble ticket that is raised during the acceptance-testing period.

7.3.14 When any fault, identified through Canada's acceptance testing, has been reported cleared by the Contractor, Canada will have an additional ten FGWDs to complete further acceptance testing. Any further service implementation fault reported within this period will restart the 10 FGWD period to allow Canada to complete acceptance-testing.

7.3.15 The billing start date for services that meet Canada's acceptance test is retroactive to the date that the last trouble ticket is cleared. In the case where Canada has raised a trouble ticket and is determined not to be the Contractor's implementation fault; the billing start date will be retroactive to the SOCN or CSDD, whichever is later.

7.3.16 If no trouble ticket is raised within the 10 FGWDs of the receipt of the SOCN then the billing start date will be retroactive to when the Contractor completed its acceptance test as stated in the SOCN or the CSDD, whichever is later.

7.3.17 The Contractor must provide 48 hours advance notice to Canada when Contractor access is required on Government of Canada premises in order to complete a Service Order.

7.3.18 The Contractor must provide the circuit number and configuration information 5 FGWDs prior to the CSDD to Canada.

Service Order (SL-SOR)	SDI
One-time Charges (modifying): • For Modifying the Committed Throughput on 10 Gbps Access • One-time charge for Modifying the DDoS Bandwidth Capacity • One-time charge for DDoS protection from Additional Attack Stream	5 FGWDs

One-time Charge (Re-locate) facilities exist: • For the relocation of circuits as and when requested Adding new or relocating a circuit to a new location where the Contractor's service facilities exist and the ordered access type is supported.	20 FGWDs
One-time Charge (Re-locate) facilities do not exist: • For the relocation of circuits as and when requested Adding new or relocating a circuit to a new location where the Contractor's service facilities do not exist but can be built and delivered.	60 FGWDs

Table 4 - Service Delivery Interval (SDI) Requirements

7.4 Service Order Amendment

7.4.1 Service Order Amendment means: an amendment to a Service Order approved by the Contracting Authority and issued to the Contractor.

7.4.2 Service Order Amendment

7.4.2.1 Canada may, for any reason, reduce or add to the Work which has been ordered in a Service Order by issuing a Service Order Amendment. If the Service Order Amendment reduces the Work, this reduction will take effect 7 calendar days after issuance of the Service Order Amendment. Canada will pay the Contractor for the Work in the amended Service Order, in accordance with the basis and method of payment provisions of the Contract.

7.4.2.2 If an amendment is required by Canada, a Service Order Amendment will be issued and sent to the Contractor. Whether or not to issue a Service Order Amendment is entirely within Canada's discretion.

7.5 Minimum Work Guarantee

7.5.1 In this clause, "**Minimum Work Guarantee**" means $75,000.00.

7.5.2 The Contractor must perform the Work described in the Contract as and when requested by Canada during the Contract Period. Canada's obligation under the Contract is to request Work in the amount of the Minimum Work Guarantee or, at Canada's option, to pay the Contractor at the end of the Contract in accordance with paragraph (7.5.3). In consideration of this obligation, the Contractor agrees to stand in readiness throughout the Contract Period to perform the Work described in the Contract.

7.5.3 If Canada does not request work in the amount of the Minimum Work Guarantee during the Contract Period, Canada must pay the Contractor the difference between the Minimum Work Guarantee and the price of the Work performed.

7.5.4 Canada will have no obligation to the Contractor under this clause if Canada terminates the Contract in whole or in part for default.

7.6 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (http://ccua-sacc.pwgsc.gc.ca/pub/acho-eng.jsp) issued by Public Works and Government Services Canada. All references contained within the General Conditions or Supplementary General Conditions to the Minister of Public Works and Government Services will be interpreted as a reference to the minister presiding over Shared Services Canada and all references to the Department of Public Works and Government Services will be interpreted as Shared Services Canada.

7.6.1 **General Conditions:**

7.6.1.1 2035 (2013-03-21), General Conditions - Higher Complexity - Services, apply to and form part of the Contract. These General Conditions are amended as follows:

Section 2 of the General Conditions is amended as follows: delete "Pursuant to the *Department of Public Works and Government Services Act*, S.C. 1996, c.16"

7.6.1.2 The text under Subsection 04 of Section 41 – Code of Conduct and Certifications 2035 (2013-03-21), General Conditions - Higher Complexity - Services, referenced above is replaced by:

4. 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.

7.6.2 **Supplemental General Conditions:**

The following Supplemental General Conditions:

7.6.2.1 4005 (2012-07-16), Supplemental General Conditions - Telecommunications Services and Products;

apply to and form part of the Contract.

7.7 Security Requirement

7.7.1 The contractor must, at all times during the performance of the Contract, Standing Offer or Supply Arrangement maintain a valid Designated Organization Screening (DOS) WITH Information Technology Security issued by Public Works and Government Services Canada – Industrial Security Program.

The contractor and/or its employees must EACH maintain a valid Reliability Status issued by Public Works and Government Services Canada – Industrial Security Program.

The contractor must maintain a valid Document Safeguarding Capability (DSC) at the Protected A level issued by Public Works and Government Services Canada – Industrial Security Program.

The contractor and/or its employees MUST NOT remove any Protected B, C 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 B, C 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) Justice Canada – Security of Information Act (Latest Edition);
b) Industrial Security Manual (Latest Edition).

7.7.2 **General Security Measures Surrounding Transmission of Sensitive Data**

7.7.2.1 The telecommunications services provided under the Contract will be used for the transmission of Government of Canada data of various kinds, including secure communications (at various security classification levels), privileged communications (such as Cabinet confidences and solicitor-client communications), and otherwise sensitive communications (including transmissions containing personal information of Canadians and proprietary or confidential information of third parties, such as suppliers).

7.7.2.2 The Contractor acknowledges that Canada requires, and the Contractor guarantees that, the telecommunications services provided under the Contract is and will be the subject of robust, comprehensive security measures that evolve as security threats and technologies evolve, so that the security measures in use are updated throughout the Contract Period, in order to achieve the highest possible levels of data integrity, availability, and confidentiality.

7.7.2.3 The Contractor must implement any reasonable security or protection measures requested by Canada from time to time, within a reasonable timeframe agreed to with Canada. The parties agree that reasonableness will be determined based on the severity of the threat to the integrity, availability and confidentiality of Canada's data and communications.

7.7.3 **Security Clearance**

7.7.3.1 The Contractor acknowledges that Canada may specify some equipment or networks as security sensitive and select a security classification in which case only security cleared employees and contractors may work on the system. Non-cleared persons may only assist in working on the system but not actually control or load software.

7.7.3.2 Remote access to some systems may be permitted, but all keystrokes and uploaded software must be copied and kept as evidence for forensic purposes, if ever required.

7.7.3.3 Upon arriving at Canada's premises, all Contractor and subcontractor personnel (which have been pre-approved by the Contracting Authority), must be able to provide proof of employment (such as a badge issued by the Contractor or the approved subcontractor) and their security clearance status must be ascertained from a trusted source;

7.7.3.4 Individuals, although not having access to CLASSIFIED information or assets, may occupy positions that are deemed to be critical to the national interest. This includes personnel who have privileged access that give them the capability to effect major disruption or damage to critical systems. These individuals are to be security screened and granted a Security Clearance to a minimum of SECRET. Examples include technical or operational personnel, including network or system administrators or managers, who directly control the most sensitive and critical functionality such as monitoring, detection, backup and recovery information, testing and installation of security patches, configuration changes to security hardware and software, responding to security incidents etc.
NOTE: additional access controls are also required such as segregation of duties to assure that no individual has over-broad access to the most sensitive functionality. Secure audit records must be available to ensure such access may be auditably linked to a specific individual.

7.7.3.5 The Contractor acknowledges that Canada may, at any time, refuse access to its premises to any individual. If that individual meets the security clearance requirements for the type of work being performed, but Canada refuses to provide any necessary access to that individual, any time described in the Contract for completing the portion of the Work to be performed by that individual will not start until Canada has informed the Contractor that access has been granted to that individual. Canada may advise the Contractor of the reason for denying access, but may also choose not to do so if Canada, in its discretion, has determined that there are security reasons for not disclosing the reason.

7.7.3.6 The Contractor must obtain the required security clearance for all of its personnel before contract award. After contract award, it is the Contractors sole responsibility to ensure that it has a sufficient complement of personnel to complete the Work who are cleared at the level required by the Contract.

7.7.3.7 The Contractor acknowledges that Canada may revoke an individual's security clearance at any time.

7.7.4 **Subcontracting**

7.7.4.1 Despite the General Conditions, none of the Work may be subcontracted (even to an affiliate of the Contractor) unless the Contracting Authority has first consented in writing. In order to seek the Contracting Authority's consent, the Contractor must provide the following information:

7.7.4.1.1 the name of the subcontractor;

7.7.4.1.2 the portion of the Work to be performed by the subcontractor;

7.7.4.1.3 the Designated Organization Screening or the Facility Security Clearance (FSC) level of the subcontractor as required by the work;

7.7.4.1.4 if requested, the security clearance status of individuals employed by the subcontractor who will require access to Canada facilities;

7.7.4.1.5 completed sub-SRCL signed by the Contractors Company Security Officer for CISD completion; and

7.7.4.1.6 any other information required by the Contracting Authority.

7.7.5 **Network Diagram**

7.7.5.1 Within 30 calendar days of Contract award, the Contractor must deliver a draft network diagram to the Technical Authority that, at a minimum, addresses the following:

7.7.5.1.1 physical and logical network topology, depicting the nodes and connections amongst nodes in the network; and

7.7.5.1.2 details of the nodes in the network, protocols, bandwidths, etc.

7.7.5.2 The Contractor must provide an updated network diagram to Canada 3 FGWD after any change which must reflect all changes made to the network. Even when there are no changes, the contractor is required to re-issue the Network Diagram with new dates at least quarterly within 2 weeks of the end of each reporting period.

7.7.5.3 The Contractor acknowledges that the network diagram is not proprietary to the Contractor.

7.7.6 **Location of Databases, Network Traffic Routing, and Data**

7.7.6.1 The Contractor must ensure that all the databases containing any information related to the Work (including billing and/or call detail information) or data are located in Canada.

7.7.6.2 The Contractor must ensure that all databases on which any data relating to this Contract is stored/archived are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases.

7.7.6.3 The Contractor must ensure that all data relating to this Contract is accessed and processed only in Canada or in an alternate jurisdiction approved by the Contracting Authority under paragraph (7.6.8.1 above).

7.7.6.4 The Contractor must ensure that all domestic network traffic (meaning traffic initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada.

7.7.7 **Network Connectivity and Access Control**

7.7.7.1 The Contractor must safeguard the network and all databases including Canada's data or information about Canada at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality. To do so, at a minimum, the Contractor must:

7.7.7.1.1 control access to all databases on which any data relating to this Contract is stored so that only individuals with the security clearance required by the Contract, and who also require access to the information in order to perform the Contract, are able to access the database;

7.7.7.1.2 ensure that passwords or other access controls are provided only to individuals who require access to perform the Work and who have the security clearance issued by CISD at the level required by the Contract; and

7.7.7.1.3 safeguard any database or computer system on which Canada's data is stored from external access using methods that are generally used, from time to time, by prudent public and private sector organizations in Canada in order to protect highly secure or sensitive information.

7.7.7.1.4 The Contractor shall demonstrate they follow sound security design and implementation practices using a formal security risk management process such as the ITSG-33, “IT Security Risk Management: A Lifecycle Approach” and as a result shall provide security assessment and assurance evidence to validate that:

7.7.7.1.4.1 (1) The appropriate security controls are selected to address applicable business needs for security, best security practices designed to mitigate vulnerabilities to threats; and

7.7.7.1.4.2 (2) Such controls are implemented effectively within the operational environment.

7.7.7.2 Development, testing live or management networks must be segregated from each other and from Canada’s existing networks.

7.7.7.3 Unless requested by the Technical Authority, the Contractor must disable any TCP/UDP listening ports on any equipment deployed on Canada’s network or on the Contractors network infrastructure or backbone with which Canada’s network is interconnected. Strong access control methods must be in place for all ports that are open for network management purposes.

The Contractor must maintain an audit log that automatically records all attempts to access Canada’s network, as well as any databases that include Canada’s data or information maintained by the Contractor about Canada (such as billing information and call detail information). Every action, transaction or business function performed on the Contractors network, systems, or databases relating to the Contract must be traceable to an individual user or account (by ensuring that user identifiers and accounts are unique and cannot be shared or transferred from one individual to another).

7.7.8 Network Management Protocols

7.7.8.1 The Contractor must ensure that the equipment/all the components that form part of the system used to deliver the network services can be managed using secure protocols.

7.7.8.2 If the Contractor is using management servers that have a configurable level of security or encryption, the Contractor must disable all levels other than the highest level of security and/or encryption.

7.7.8.3 The Contractor must not use protocols that send clear text usernames or passwords over the network.

7.7.8.4 The Contractor must not use (and must disable any) protocols that cannot pass through session-aware firewalls.

7.7.8.5 Canada will not consider an otherwise insecure protocol to be secure as a result of the use of tunnelling techniques such as port forwarding or Internet Protocol Security (IPSec).

7.7.8.6 The Contractor must implement encryption protocols identified by Canada and must disable all encryption protocols not approved by Canada.

7.7.9 Vulnerability Assessment and Management

7.7.9.1 The Contractor must provide to the Technical Authority timely information about vulnerabilities (i.e., any weakness, or design deficiency, identified in any equipment provided under the Contract/any component that forms part of the system used to deliver the network services that would allow an unauthorized individual to compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications it hosts.

7.7.9.2 Where any vulnerability is caused by equipment manufactured by or software code written by the Contractor or one of its subcontractors, the Contractor must immediately remedy the vulnerability at its own cost.

7.7.9.3 Where any vulnerability is caused by equipment manufactured by or software code written by a third party (other than a subcontractor), in addition to notifying the Technical Authority about the vulnerability as soon as the Contractor learns of it, the Contractor must implement any upgrades, patches or other fixes within a timeframe acceptable to Canada once they are made available by

the manufacturer or software publisher, at the Contractors own cost, unless the Technical Authority waives this requirement (in respect of a specific upgrade, patch or fix) in writing.

7.7.10 **Security Monitoring and Incident Reporting**

7.7.10.1 The Contractor must monitor the network for abnormal or suspicious activities, such as odd work hours, unnecessary requests for code or data, abnormal data movements, or excessive use of systems or resources.

7.7.10.2 The Contractor must immediately report to the Technical Authority and CISD any incidents relating to the security of Canada's network, or the Contractors network infrastructure or backbone, or Canada's data, if it impacts Canada, including but not limited to those incidents listed in (7.6.12.1). For example, any unauthorized access or attempt to gain unauthorized access must immediately be reported. Also, the discovery of any virus or malicious code and/or the installation of any unauthorized software code on any equipment must immediately be reported.

7.7.10.3 The Contractor agrees to cooperate fully with Canada in the investigation of any security incident

7.7.11 **Security Audit**

Canada may audit the Contractors compliance with the security requirements included in the Contract at any time. If requested by the Contracting Authority, the Contractor must provide Canada (or Canada's authorized representative) with full access to its premises, its network, and all databases storing Canada's data or data related to the Contract at all reasonable times. If Canada identifies any security deficiencies during an audit, the Contractor must immediately correct the deficiencies at its own expense.

7.8 Supply Chain Security

7.8.1 At any time during the Contract, if the Contractor proposes introducing new commercial products, that were not on the IT Products List approved by Canada, on Canada's network or on the Contractor's own or 3rd party infrastructure or backbone that will be interconnected with Canada's network, the Contractor must first obtain the written approval of the Technical Authority. Canada reserves the right to refuse new commercial products, propose new safeguards and to independently validate and approve the commercial products.

7.8.2 At any time, if Canada notifies the Contractor that any given manufacturer or OEM is no longer considered a trusted manufacturer or OEM (i.e. un-trusted), the Contractor (and its subcontractors) must immediately cease deploying equipment made by that manufacturer or OEM in Canada's network and in any infrastructure or backbone of the Contractor that will interconnect with Canada's network. For already deployed equipment, the Contractor has to identify and/or remove equipment made by that manufacturer or OEM in Canada's network and in any infrastructure or backbone of the Contractor that will interconnect with Canada's network. If Canada requests a change as per this section the Contractor shall be entitled to an equitable adjustement.

7.8.3 If the Contractor becomes aware that any third party (other than a subcontractor) is deploying un-trusted equipment on its network, the Contractor must immediately notify the Technical Authority.

7.8.4 **Change in Control**

For the purposes of the General Conditions 2035 (2013-03-21), Higher Complexity - Services, the term "assignment" includes but is not limited to a change in control if the Contractor is a corporation (whether a direct or indirect change in the effective control of that corporation, whether resulting from a sale, encumbrances, or other disposition of the shares of by any other means).

7.9 Contract Period

7.9.1 **Contract Period**: The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, which includes:

7.9.1.1 The "**Initial Contract Period**", which begins on the date the Contract is awarded and ends 3 year(s) later; and

7.9.1.2 The period, during which the Contract is extended, if Canada chooses to exercise any options set out in the Contract.

7.9.2 **Option to Extend the Contract**:

7.9.2.1 The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 1 additional 1-year period 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.

7.9.2.2 Canada may exercise this option at any time by sending a written notice to the Contractor at least 30 calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced, for administrative purposes only, through a contract amendment.

7.10 Authorities

7.10.1 Contracting Authority

The Contracting Authority for the Contract is:

Name: Mark Hall
Title: Supply Specialist
Department: Shared Services Canada
Directorate: Information Technology Shared Services Procurement Directorate
Address: 11 Laurier, Gatineau, QC
Telephone: 819-956-0251
Facsimile: 819-956-9191
E-mail: mark.hall@ssc.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

7.10.2 Technical Authority

The Technical Authority for the Contract is:

<To be inserted at Contract Award>

The Technical Authority 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.

7.10.3 Contractor's Representative

<To be inserted at Contract Award>

7.11 Payment

7.11.1 Basis of Payment

7.11.1.1 **Internet Interconnection Services (IIS):** For providing Internet Interconnection Services, in accordance with the Contract, Canada will pay the Contractor a monthly recurring cost as set out in Annex B, GST/QST/HST extra.

7.11.1.2 **Modifying the Committed Rate on IIS:** For modifying the Committed Rate on 10 Gbps Access, in accordance with the Contract, Canada will pay the Contractor a one-time Non-Recurring Installation Price (NRIC), as set out in Annex B, GST/QST/HST extra.

7.11.1.3 **DDoS Protection:** For providing Anti-DDoS scrubbing service for up to 5 on-going Attack Streams, in accordance with the Contract, Canada will pay the Contractor a monthly recurring cost as set out in Annex B, GST/QST/HST extra.

7.11.1.4 **Additional DDoS Attack Streams:** For providing additional DDoS Protection from Additional Attack Streams over and above the 5 on-going Attack Streams in 7.10.1.3 above, in accordance with the Contract, Canada will pay the Contractor a monthly recurring cost per additional attack stream, as set out in Annex B, GST/QST/HST extra.

7.11.1.5 **One-Time Non-Recurring Installation Charges (NRIC):** One-time charges are permitted for the relocations of existing IIS or for additional IIS installations only if one or more of the following criteria's apply:

(i) Access facilities (including conduit between the property line and the building) are required because no facilities exist, or existing facilities are either at full capacity or damaged beyond repair;

(iv) Relocation of existing IIS where the actual terminating equipment will be physically relocated and reused at the new site.

7.11.1.6 **Taxes:** Canada will pay the Contractor GST, QST or HST as applicable.

7.11.1.7 Prorating for Partial Months: Where the Services are accepted or terminated on a day other than the first or last day of the month, the Contractor must prorate the applicable monthly rate based on the number of in-service days in a 30-day month.

7.11.1.8 Where the Contract includes Work for which there are no separate line items in the basis of payment or the Annex C - IIS Pricing, the prices for this Work is included in the rates/prices for the Services as detailed in Annex C - IIS Pricing.

7.11.1.9 Transitioning Services to the Contractor - implementation phase

7.11.1.9.1 The amount payable to the Contractor for the Services included in any Service Order will be zero at the beginning of the implementation phase of the Service and will increase incrementally with each billing period as the Contractor makes the Services operational and these Services are accepted by Canada.

7.11.1.10 Transition Services at the end of the Contract Period

7.11.1.10.1 The amount payable to the Contractor for the Services included in any Service Order will decrease in accordance with the Services terminated during each billing period. There must be no cost to Canada or charges of any type or for any reason associated with the Contractor's time and effort in phasing out the Services during the Contract termination phase.

7.11.1.11 **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.

7.11.1.12 **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 goods or services in these amounts. Any commitment to purchase specific amounts or values of goods or services is described elsewhere in the Contract.

7.11.2 **Limitation of Expenditure**

7.11.2.1 The Contractor will be reimbursed for the costs reasonably and properly incurred in the performance of the Work specified in the authorized Service Order (SO), as determined in accordance with the Basis of Payment detailed above, to the limitation of expenditure specified in the authorized Service Order (SO).

7.11.2.2 Canada's liability to the Contractor under the authorized SO must not exceed the limitation of expenditure specified in the authorized SO. Customs duties are included and Goods and Services Tax Quebec Sales Tax or Harmonized Sales Tax is extra, if applicable.

7.11.2.3 No increase in the liability of Canada or in the price of the Work specified in the authorized SO 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 authorized, in writing, by the Contracting Authority before their incorporation into the Work.

7.11.3 **Method of Payment for Service Order - Monthly Payment**

7.11.3.1 H1008C (2008-05-12), Monthly Payment

7.11.4 **Method of Payment for Service Order - Single Payment**

7.11.4.1 H1000C (2008-05-12), Single Payment

7.11.5 **Payment Credits**

The Contractor must provide credits to Canada if it does not meet the requirements of Service Levels, Service Delivery and Response Times as detailed in Annex A (Statement of Work) or elsewhere in the Contract. The Contractor must include service credits in the monthly invoice that immediately follows the month in which service credits accrue. The applicable credits must be calculated as a percentage of the total monthly invoice for the impacted service in accordance with the methods described below.

7.11.5.1 **Credits for Failure to Meet Internet and Anti-DDoS Availability Level:** If the Contractor exceeds the Maximum Service Outage Time (SL-MSOT) for Internet and Anti-DDoS services as described in Annex A SOW, in any given month, Canada will be entitled to credit as defined in Table 1 below.

Accumulated Monthly Outage	Service Credit
Outage <= 40 min	**0%**
40 min < Outage <= 3 hrs	10%
3 hrs < Outage <= 4.5 hrs	25%
Outage > 4.5 hrs	50%

Table 1: Service Credits

7.11.5.2 **Credits for Failure to Meet Minimum Service Level for Data throughput, SL-PTD and SL-DPL:** If the Contractor does not meet the Minimum Service Levels described in Annex A SOW, in any given month, Canada will be entitled to credit as defined in Table 2.

Total Service Hours Failed per Month	Service Credit
2 - 3 hrs Failed	10%
4 - 6 hrs Failed	25%
>6 hrs Failed	50%

Table 2: Service Credits

7.11.5.3 **Credits for Failure to Meet Service Order Response Times (SL-SOR):**

7.11.5.3.1 The Contractor must provide a Service Credit as a percentage of the total monthly service charge for the associated Service Order for each business day that the Committed Service Delivery Date (CSDD) is not met as shown in Table 3 below.

Service Credit = (Total monthly cost of the associated Service) x (Service Credit Percentage) x (number of FGWDs over CSDD)

7.11.5.3.2 The Contractor must calculate the applicable Service Credit for a new Service Order Request, where they are in default in meeting the Committed Service Delivery Date, against the total monthly amount for this new service for the first full month following the successful completion of the Service Order Request.

Service Order (SL-SOR)	Service Credit (% per business day over CSDD for the impacted service)
One-time Charges (modifying): • For Modifying the Committed Throughput on 10 Gbps Access • One-time charge for Modifying the DDoS Bandwidth Capacity • One-time charge for DDoS protection from Additional Attack Stream	10%
One-time Charge (Re-locate) facilities exist: • For the relocation of circuits as and when requested Adding new or relocating a circuit to a new location where the Contractor's service facilities exist and the ordered access type is supported.	10%
One-time Charge (Re-locate) facilities do not exist: • For the relocation of circuits as and when requested Adding new or relocating a circuit to a new location where the Contractor's service facilities do not exist but can be built and delivered.	10%

Table 3: Service Delivery Interval Service Credits

7.11.5.4 **Corrective Measures**: If credits are payable under this Article for 2 consecutive months or for 3 months in any 12-month period, the Contractor must submit a written action plan describing measures it will implement or actions it will undertake to eliminate the recurrence of the problem. The Contractor will have 5 working days to deliver the action plan to Canada and the Contracting Authority and 20 working days to rectify the underlying problem.

7.11.5.5 **Termination for Failure to Meet Minimum Availability Level:** In addition to any other rights it has under the Contract, Canada may terminate the Contract for default in accordance with the General Conditions by giving the Contractor 3 months' written notice of its intent, if any of the following apply:

7.11.5.5.1 the total amount of credits for a given monthly billing cycle reach a level of 10%; or

7.11.5.5.2 the corrective measures required of the Contractor described above are not met.

This termination will be effective when the three-month notice period expires, unless the Contractor has sustained the Minimum Availability Level during those months.

7.11.5.6 **Credits Apply during Entire Contract Period**: The Parties agree that the credits apply throughout the Contract Period, including during implementation.

7.11.5.7 **Credits represent Liquidated Damages**: The Parties agree that the credits are liquidated damages and represent their best pre-estimate of the loss to Canada in the event of the applicable failure. No credit is intended to be, nor will it be construed as, a penalty.

7.11.5.8 **Canada's Right to Obtain Payment**: The Parties agree that these credits are a liquidated debt. To collect the credits, Canada has the right to hold back, draw back, deduct or set off from and against any money Canada owes to the Contractor from time to time.

7.11.5.9 **Canada's Rights & Remedies not Limited**: The Parties agree that nothing in this Article limits any other rights or remedies to which Canada is entitled under the Contract (including the right to terminate the Contract for default) or under the law generally.

7.11.5.10 **Audit Rights**: The Contractor's calculation of credits under the Contract is subject to verification by government audit, at the Contracting Authority's discretion, before or after payment is made to the Contractor. The Contractor must cooperate fully with Canada during the conduct of any audit by providing Canada with access to any records and systems that Canada considers necessary to ensure that all credits have been accurately credited to Canada in the Contractor's invoices. If an audit demonstrates that past invoices contained errors in the calculation of the credits, the Contractor must pay to Canada the amount the audit reveals was required to be credited to Canada, plus interest, from the date Canada remitted the excess payment until the date of the refund (the interest rate is the Bank of Canada's discount annual rate of interest in effect on the date the credit was first owed to Canada, plus 1.25% per year). If, as a result of conducting an audit, Canada determines that the Contractor's records or systems for identifying, calculating or recording the credits are inadequate, the Contractor must implement any additional measures required by the Contracting Authority.

7.11.6 **No Responsibility to Pay for Work not performed due to Closure of Government Offices**

7.11.6.1 Where the Contractor, its employees, subcontractors, or agents are providing services on government premises under the Contract and those premises are inaccessible because of the evacuation or closure of government offices, and as a result no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if there had been no evacuation or closure.

7.11.6.2 If, as a result of any strike or lock-out, the Contractor or its employees, subcontractors or agents cannot obtain access to government premises and, as a result, no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if the Contractor had been able to gain access to the premises.

7.12 Invoicing Instructions

7.12.1 The Contractor must submit invoices in accordance with the information required in the General Conditions.

7.12.2 The Contractor's invoice must include a separate line item for each subparagraph in the Basis of Payment provision.

7.12.3 By submitting invoices, the Contractor is certifying that the services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.

7.12.4 The Contractor must provide the original of each invoice to the following address:

Shared Services Canada
Telecom Accounts Payable Office
Place du Portage, Phase III, Section 5A2
11 Laurier Street
Gatineau, Québec, K1A 0S5

7.12.5 The Contractor must also provide an electronic copy in Portable Document Format (PDF) of all invoices to the Contracting Authority.

7.12.6 In addition to the monthly invoice, the Contractor must submit a Billing Detail File in Portable Document Format (PDF), as per Annex E, Format of Billing Detail File.

7.12.7 The 'Billing Detail File' must be submitted on a monthly basis and must contain all data that was processed during the prior billing period (including any resubmitted charges from the previous billing periods). The amount on the hard copy summary invoice(s) must equal the total on the 'Billing Detail File', and in case of a discrepancy, the Billing Detail File will take precedence. The amount that will be paid is the total amount on the file less any transactions that were rejected.

7.13 Certifications

7.13.1 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 entire Contract Period. 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, under the default provision of the Contract, to terminate the Contract for default.

7.14 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in _____. *<To be inserted at Contract Award>*

7.15 Priority of Documents

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

7.15.1 section 02 of Supplemental General Conditions 4005 (Telecommunications Services and Products) entitled “Termination Rights Associated with Breach of Telecommunications Warranties and Representations”;

7.15.2 _____ (collectively referred to as the “**Tariff**”)

Note to Bidders: This clause will not be included in any resulting contract if the Contractor’s bid is not subject to any tariffs.

7.15.3 these Articles of Agreement, including any individual SACC clauses incorporated by reference in these Articles of Agreement;

7.15.4 Supplemental General Conditions 4005, except 02 which takes priority as set out above under sub-paragraph 7.15.1;

7.15.5 general conditions 2035 (2013-03-21), General Conditions - Higher Complexity - Services;

7.15.6 Annex A, Statement of Work;

7.15.7 Annex B, IIS Pricing;

7.15.8 Annex C, Security Requirements Check List;

7.15.9 Annex D, Access to Crown Property for Telecommunications Services;

7.15.10 Annex E, Billing Format File

7.15.11 the signed Service Orders;

7.16 Foreign Nationals (Canadian Contractor)

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

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

7.17 Foreign Nationals (Foreign Contractor)

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

7.18 Insurance Requirements

7.18.1 SACC Manual clause G1005C (2008-05-12), Insurance

7.19 Limitation of Liability - Information Management/Information Technology

7.19.1 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 Article, even if it has been made aware of the potential for those damages.

7.19.2 **First Party Liability**:

7.19.2.1 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:

7.19.2.1.1 any infringement of intellectual property rights to the extent the Contractor breaches the section of the General Conditions entitled "Intellectual Property Infringement and Royalties";

7.19.2.1.2 physical injury, including death.

7.19.2.2 The Contractor is liable for all direct damages affecting real or tangible personal property owned, possessed, or occupied by Canada.

7.19.2.3 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.

7.19.2.4 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 subparagraph 2.1.1 above.

7.19.2.5 The Contractor is also liable for any other direct damages to Canada caused by the Contractor in any way relating to the Contract including:

7.19.2.5.1 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

7.19.2.5.2 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 by Canada either in whole or in part for default, up to an aggregate maximum for this subparagraph 2.5.2 of the greater of 0.25 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the cell 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 $1M.

7.19.2.5.3 In any case, the total liability of the Contractor under subparagraph 2.5 will not exceed the total estimated cost (as defined above) for the Contract or $1M, whichever is more.

7.19.2.6 If Canada's records or data are harmed as a result of the Contractor's negligence or wilful 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.

7.19.3 **Third Party Claims**:

7.19.3.1 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.

7.19.3.2 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 Sub-article 3.1, 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.

7.19.3.3 The Parties are only liable to one another for damages to third parties to the extent described in this Sub-article 3.

7.20 Joint Venture Contractor

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

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

7.20.2.1 _____ has been appointed as the “representative member” of the joint venture Contractor and has fully authority to act as agent for each member regarding all matters relating to the Contract;

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

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

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

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

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

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

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

7.21 Telecommunications Services

7.21.1 **Improvements to the Service**: The Contractor agrees to advise the Technical Authority of all improvements that affect the Services, including technological, administrative, commercial or other types of improvements. The Contractor agrees to offer all improvements it is offering to any other customer as part of its standard services at no additional charge to Canada. Any other improvements must only be provided following approval in writing by the Contracting Authority. The price of these other service improvements will be negotiated on a case-by-case basis. These improvements may include, among other things, discounts resulting from aggregating certain services or discounted pricing for additional capacity.

7.22 Installation of Telecommunications Facilities on Canada's Property

Canada's property, facilities, equipment, documentation, and personnel are not automatically available to the Contractor. If the Contractor would like access to any of these, it is responsible for making a request to the Technical Authority. Canada will provide the Contractor with access to Canada's property for the purpose of installing telecommunications equipment and facilities (e.g., cabling) reasonably necessary for providing services to Canada under the Contract in accordance with the Annex entitled “Access to Crown Property for Telecommunications Services”. Access to certain buildings may be associated with additional security requirements. Canada has no obligation to arrange for access by the Contractor to buildings not owned by Canada and Canada will not be responsible for paying any access fees charged by any other owner.

7.23 Safeguarding Electronic Media

7.23.1 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.

7.23.2 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.

7.24 Representations and Warranties

The Contractor made statements regarding its experience and expertise in its bid that resulted in the award of the Contract. The Contractor represents and warrants that all those statements are true and acknowledges that Canada relied on those statements in awarding the Contract. 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 will 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.

7.25 Transition Services at end of Contract Period

The Contractor agrees that, in the period leading up to the end of the Contract Period, it will make all reasonable efforts to assist Canada in the transition from the Contract to a new contract with another supplier. The Contractor agrees that there will be no charge for these services.

ANNEX A

STATEMENT OF WORK

<Attached>

ANNEX B

IIS PRICING

<To be inserted at Contract Award>

ANNEX D

ACCESS TO CROWN PROPERTY FOR TELECOMMUNICATIONS SERVICES

1. ACCESS

1.1. Equipment Area and Use

1.1.1. Canada grants to the Contractor, for the Contract Period, access:

1.1.1.1. To install, maintain, operate, repair, replace, and remove, at the Contractor's sole expense and risk, "**Communications Equipment**" (defined as the cabinets, racks and other electronic equipment specified in Schedule A), on and in the Equipment Area (as described in Schedule B) on the lands and buildings defined in the Contract for the supply of telecommunications services (the "**Property**");

1.1.1.2. To install, maintain, operate, repair and replace, at the Contractor's sole expense and risk, certain "**Connecting Equipment**" (the cables, conduits, inner ducts, connecting hardware and other passive equipment, as specified and described in Schedule A), together with the right to pull that Connecting Equipment through the Property's "**Entrance Link**" (defined as the core sleeve penetration through the Property foundation) and through other "**Property Communications Spaces**" (defined as the telecommunications pathways necessary to reach from the Entrance Link to the Contractor's Equipment Area in the Building and from the Equipment Area to the Contractor's customers, as may be necessary to provide telecommunications services to the Contractor's customers, as designated and approved by Canada). The Contractor's Communications Equipment and the Contractor's Connecting Equipment are collectively referred to in these provisions as the "**Contractor's Equipment**", and the Entrance Link, Property Communications Spaces and Equipment Area are collectively referred to as the "**Access Area**";

1.1.1.3. To use Canada’s existing telecommunications wiring, if available, consistent with the most current CRTC guidelines (or, if there are no CRTC guidelines, consistent with best practices within the industry) for use of such wiring, in order to connect the Contractor's Equipment to the users located in the Property. Canada may permit use of existing Property Entrance Link and existing Property wiring only to the extent that Canada has the possession of and authority to allow such use of these facilities. In no event will Canada be obligated to provide the Contractor with use of facilities to the extent that it does not own, control, or have authority to allow that usage; and

1.1.1.4. For right of ingress and egress for the Contractor's employees, servants and agents, customers and invitees, and the use of the elevators, entrances lobbies, hallways, stairways, driveways, common loading and stopping Equipment Areas in and about the Property, the "**Common Equipment Areas**".

1.1.2. Canada will provide floor space in the Property and in a location designated by Canada and shown shaded on the floor plan attached as Schedule B to this Annex (the "**Equipment Area**"). Canada has the right, in its sole discretion, to reasonably limit the type, size and location of the Contractor's Equipment located in the Property.

1.1.3. The access granted is not exclusive. Canada has the right to grant, renew or extend similar rights to others.

1.1.4. The Contractor must use the Access Area solely for the purpose of providing Canada with telecommunications services ("**Permitted Use**"). The Contractor is expressly forbidden to serve other properties or other users from this location without the prior written permission of Canada.

Additional fees and conditions may be required, as agreed to between the Parties, for using the Contractor's Equipment Area as a service point for other properties outside the Property.

1.1.5. The Contractor acknowledges that the Contractor does not and must not claim at any time any interest or estate of any kind or extent whatsoever in the Property, Property Communications Spaces, or Equipment Area by virtue of these provisions or the Contractor's use of the Property, Property Communications Spaces or Equipment Area. The Contractor further acknowledges that in no event will the relationship between Canada and the Contractor be considered to be a landlord-tenant relationship and that in no event will the Contractor be entitled to avail itself of any rights afforded to tenants under the laws of the Province that govern the Contract.

1.2. Inspection

Canada makes no warranty or representation that the Access Area or the Property is suitable for the Contractor's use. The Contractor therefore acknowledges and agrees that access to the Equipment Areas are being provided on an "as is" basis in the then-existing condition. There is no covenant, agreement, promise, representation, warranty, condition or undertaking, whether expressed or implied, collateral or otherwise, whether oral or written, by or binding on Canada or any agent or any representative or any other person with respect to any zoning, use, development, alteration or decoration, or installation of equipment or fixtures in or in connection with the Access Area or any part, unless expressly set forth in these provisions.

1.3. Contractor's Warranty

The Contractor warrants that the operation of the Contractor's Equipment will not interfere with the operation of any existing radio or telecommunication equipment installed in the Property, nor will the operation of the Contractor's Equipment interfere with the use and enjoyment of the Property by any other occupant of the Property and their employees, customers and invitees. If the operation of the Contractor's Equipment does interfere with the operation of any existing radio or telecommunication equipment installed in the Property, and if the Contractor fails to remedy this condition within 24 hours after notice by Canada, then Canada may, in addition to its rights under Section 4.2 of these provisions, enter into the Equipment Area and remedy the condition giving rise to the interference and the Contractor must pay to Canada the cost of doing so, plus a sum equal to 15% of the cost representing Canada’s overhead.

1.4. Telecommunication Management

1.4.1. The Contractor acknowledges and agrees that Canada will have the right, but not the obligation, to co-ordinate, restrict, enforce and approve all third party riser management firms who wish access to the building's risers. The Contractor acknowledges that Canada may retain a riser management firm or other third party manager to co-ordinate, supervise and approve the work of all telecommunication contractors, at Canada’s cost unless otherwise specified in these provisions or agreed to in advance by the Contractor.

1.4.2. The Contractor recognizes that Canada may desire to provide access to existing and future telecommunications service providers of Property tenants, and Canada may consider it desirable to achieve this objective through shared usage of some or all of the Property Communications Spaces. Canada may purchase from the Contractor those portions of the Contractor's Connecting Equipment (excluding wiring) that the Crown, in its sole discretion, determines is necessary to incorporate efficiencies in the Property Communication Spaces. Canada acknowledges that the Contractor may be bound by service agreements with clients located in the Property to retain ownership of its Connecting Equipment and cannot be compelled to sell those portions of the Contractor's Connecting Equipment. The purchase price of those portions of Contractor's Connecting Equipment will be determined on the basis of their undepreciated capital cost at the time of Canada’s written notice to purchase. In connection with any such purchase, Canada agrees to negotiate the terms of the Contract to allow for continued use of the sold Connecting Equipment, at a price that reflects fair market rates.

1.4.3. If Canada wishes to purchase any wiring that forms part of the Connecting Equipment, the terms will be negotiated between Canada and the Contractor.

1.5. Access

The Contractor may only have access to the Access Area under these provisions and in accordance with the instructions of the property manager responsible for the Property. The Contractor acknowledges and agrees that its representatives or contractors may be required to obtain suitable security clearance before obtaining access to the Access Area. The Contractor may have access to the Access Areas 24 hours a day, 7 days a week as long as the Contractor provides Canada with as much prior notice as possible, and if the Contractor requires access before 8:00 a.m. or after 6:00 p.m. between Monday and Friday or at any time on a Saturday, Sunday or statutory holiday, unless Canada has agreed otherwise, the Contractor must pay an additional fee based on an agreed hourly rate as per the "Public Works Canada Services Program - Hourly Billable Rates Table" directive effective as of the date of this Access Agreement and as amended from time to time.

2. ADDITIONAL COSTS

2.1. Costs of Other Services

2.1.1. The Contractor must pay to Canada all charges for providing additional services in connection with the installation and operation of the Communications Equipment as reasonably determined by Canada from time to time. These charges may include, without limitation, any additional utility charges, charges for security, supervision, receiving, storing, handling and removal of materials and articles. If requested in writing by the Contractor, Canada will provide a cost estimate in advance of supplying or performing these services at the Contractor's cost. If Canada chooses not to provide any services to the Contractor, then they must be provided only by persons approved in writing by Canada acting reasonably.

2.1.2. Unless otherwise expressly agreed to by Canada and Contractor to the contrary, the cost of all work, materials and other services performed or supplied by Canada respecting the Equipment Area plus an administration fee of 15% on that amount must be paid by the Contractor. In addition, if Canada, acting reasonably, determines that certain other services are required, the Contractor must pay to Canada all charges for all such other services whether or not those special services were requested by the Contractor. Canada will provide reasonable notice in advance of supplying or performing special services.

2.2. Payment

The Contractor will pay to Canada, within 30 days following receipt of invoices, all amounts required to be paid by the Contractor under these provisions, failing which the Contractor will be in default under the Contract. All amounts payable by the Contractor past due will bear interest from the date on which they became due until the date of payment at the same rate as payments due by Canada to the Contractor under the General Conditions under the section entitled “Interest on Overdue Accounts”.

3. CONSTRUCTION AND MAINTENANCE

3.1. Construction

3.1.1. The Contractor, at its expense and at all times under the supervision of Canada, must install the Contractor's Equipment (if any), including any and all fittings, anchors and other materials used to secure the Contractor's Equipment to the Access Area; must prepare the Equipment Area and must carry out any Contractor's Additional Work, described in Section 3.1.3; all of which work is collectively referred to as the “**Installation Work**”. The Installation Work must be of a first class professional nature, quality and design, and is subject to Canada’s prior written approval. The

Installation Work and the Communications Equipment must be provided and installed by the Contractor in accordance with the plans, drawings and specifications submitted by the Contractor in advance, which will require Canada's prior written approval. In no event will Canada's approval of those plans be considered a representation that Contractor's Equipment will not cause interference with other systems in the Property or that Contractor's plans comply with applicable laws, rules or regulations, since that responsibility will remain with the Contractor.

3.1.2. The Installation Work must be performed: (i) at the sole cost of the Contractor; (ii) by contractors and workmen approved by Canada; (iii) in a good and workmanlike manner; (iv) in accordance with drawings and specifications approved by Canada; (v) in accordance with all applicable laws and regulations; (vi) subject to the reasonable regulations, supervision, control and inspection of Canada; and (vii) subject to such indemnification against liens and expenses as Canada reasonably requires. Upon completion of the Installation Work and any and all subsequent alterations, the Contractor must, at its expense, submit to Canada a complete set of "as-built" mechanical, electrical, architectural and structural drawings, and electronic copies, of the Equipment Area reflecting the completed work. The Contractor must pay to Canada the Crown's reasonable costs of reviewing the drawings and specifications and supervising all such work. Despite the foregoing, Canada will have the right to perform any or all of the building related Installation Work at the Contractor's cost, and the Contractor must pay to Canada the cost of this related work plus a sum equal to 15% of such cost representing the Crown's overhead, all as reasonably determined by Canada.

3.1.3. The Contractor must, at its sole cost, obtain all required permits, accesses, consents and other approvals, as the case may require, for the installation, maintenance and operation of the Contractor's Equipment. Where required by Canada, the Contractor must obtain the written assurances of a professional engineer with respect to the Installation Work conforming to all required safety measures including wind load resistance and floor load capacity.

3.1.4. For all new installations, the Contractor must label each cable placed in the telecommunications pathways, in each telephone closet through which cables pass, with identification information including, but not limited to, the Contract serial number, the floor where the cable originates and the floor where cable terminates, and any other information as may be reasonably required by Canada.

3.1.5. The Contractor will not, during construction or otherwise, block access to or in any way obstruct, interfere with or hinder the use of the Property's loading docks, the sidewalks around the Property or any of its entranceways. If this occurs, the Contractor must take corrective action as promptly as feasible, but in no event more than 24 hours following notice by Canada.

3.1.6. The Contractor may amend Schedule A, from time to time, with the prior written consent of Canada, which consent must not be unreasonably withheld, for the purpose of serving additional Property tenants. All terms and conditions of this Section 3 will apply to such circumstances. The Contractor is solely responsible for all costs for the construction of any additional facilities including, but not limited to, risers and telecom rooms, if these facilities are required to accommodate the installation of the Contractor's Equipment.

3.1.7. Canada may: (i) alter, construct improvements to, rearrange and construct additional facilities in the Property; (ii) relocate the facilities and improvements in or comprising the Property; (c) do whatever things on or in the Property are required to comply with any laws, by-laws, regulations, orders or directives affecting the Property or any part of it; and (d) do whatever other things on or in the Property as Canada determines to be advisable.

3.2. Hazardous Materials

3.2.1. The Contractor will not install or bring any hazardous substance or material onto the Property. If any hazardous materials are installed or brought into the Property by or on behalf of Contractor,

then the Contractor must cause their removal within 24 hours. If the Contractor discovers, uncovers, disturbs, or otherwise reveals any existing hazardous materials within the Property, the Contractor must immediately stop any work in progress and report its findings to Canada within 24 hours. The Contractor must not conduct any further work in the reported Equipment Area without Canada's prior written approval.

3.2.2. The Contractor will have three options upon discovery of pre-existing hazardous material and cessation of work as described above: (i) reroute its planned access route to avoid the hazardous material Equipment Areas; (ii) terminate Access according to the procedure described in Section 4; (iii) reschedule its installation work to a period after Canada has completed corrective action; however, the Contractor may terminate the right to use the Access Area by giving written notice to Crown if that corrective action has not been started and diligently pursued within 30 days after Canada receives notice of the Contractor's discovery of the hazardous materials. If (i) is not possible or (iii) causes delays in the installation work, the Contractor is released from its obligations to provide the telecommunications services to require the right to use the affected Access Area.

3.3. Maintenance and Repair

3.3.1. All maintenance, repairs and replacements of or to the Contractor's Equipment and any and all fittings, anchors and other materials used to secure the Communications Equipment on the Equipment Area must be performed by, and will be the sole responsibility of, the Contractor, at its sole expense.

3.3.2. Except for the maintenance, repairs and replacements referred to in Section 3.3.1 above, all maintenance, repairs or replacements (whether structural, major or otherwise) of or to the Access Area or any other part of the Property due to or arising from: (i) the Contractor's use of the Access Area, (ii) the installation or operation of the Contractor's Equipment, or (iii) the installation of any wiring in connection with the Contractor's Equipment, will be performed by Canada, at the Contractor's sole cost.

3.3.3. If: (i) the Property is damaged or destroyed or requires repair, replacement or alteration as a result of the act or omission of the Contractor, its employees, agents, invitees, licensees, contractors or others for whom it is in law responsible; or (ii) if Canada determines that any repairs, replacements or improvements to any part of the Property, including, without limitation, to any of the systems of the Property, are required as a result of the use of the Access Area by the Contractor, the Contractor must pay to Canada the cost of the resulting repairs, replacements, improvements or alterations.

3.3.4. If Canada determines that: (i) the presence of the Contractor's Equipment in the Property; (ii) the state of repair of the Contractor's Equipment; or (iii) the Contractor's use of the Property, creates an emergency situation, Canada will, without notice to the Contractor, take any actions that Canada determines are required to remedy the emergency and the Contractor must pay to Canada the cost of those actions, plus a sum equal to 15% of that cost (representing Canada's overhead).

4. TERMINATION

4.1. Restoration of the Equipment Area

4.1.1. Except as may be specifically provided for in this Section, the Contractor's Equipment will at all times remain the property of the Contractor. The Contractor, at the expiration or earlier termination of the right to use the Access Area, at its cost must: (i) remove the Contractor's Equipment, all trade fixtures and all of the Contractor's personal property from the Access Area, (ii) restore the Access Areas to Canada's then current Property standard (including, without limitation, the removal and disposal of any and all hazardous or toxic substances and their

containers in accordance with all applicable laws and the requirements of all authorities and all required repairs and restoration of the roof of the Property) to the extent required by Canada, and (iii) otherwise peaceably surrender and deliver up vacant possession of the Access Areas to Canada (in as good order, condition and repair as the Contractor is required under these provisions to maintain and keep the Access Area). The Contractor, at its cost, must repair any damage caused to the Property or any part of it by this removal or restoration.

4.1.2. If the Contractor does not remove its Contractor's Equipment, trade fixtures and personal property at the expiry or earlier termination of the right to use the Access Area, then, at the option of Canada and without prejudice to any other rights or remedies available to Canada, the Contractor's Equipment, trade fixtures and personal property will become the absolute property of Canada without payment of any compensation for it to the Contractor and, without notice to the Contractor, may be removed from the Access Area and sold or disposed of by Canada in the manner it considers advisable, all without any liability whatsoever to Canada. If the Contractor fails to repair any damage or complete any work, removal, disposal or restoration referred to in this section by the expiry or earlier termination of these provisions, the Contractor must pay to Canada the cost of removing and selling or disposing of such Contractor's Equipment, trade fixtures and personal property and restoring the Access Area to Canada’s then current Property standard, plus a sum equal to 15% of the cost representing the Crown's overhead.

4.1.3. The Contractor expressly acknowledges and agrees that the Contractor's obligations under Section 4.1.1 of these provisions will survive the expiry or termination of the right to use the Access Area and will not merge.

4.2. Default and Early Termination

4.2.1. If the Contractor fails to perform, observe or comply with any of: (i) the provisions other than payment by the Contractor of any costs; or (ii) the rules and regulations and amendments applicable to the Access Area, then Canada, in addition to and without limiting any of its other rights or remedies, will have the immediate right, to be exercised by written notice to the Contractor, to suspend the right to use the Access Area granted under these provisions (until such failure is remedied by the Contractor). If: (A) the Contractor fails to remedy the breach within 10 days (or such shorter period as may be provided in these provisions), or (B) if the breach cannot reasonably be remedied within 10 days or such shorter period, the Contractor fails to commence to remedy such breach within 10 days or such shorter period or thereafter fails to proceed diligently to remedy its breach, in either case after the suspension notice set forth in this Section 4.2.1, then Canada will have the further right, to be exercised by written notice to the Contractor, to terminate the right to use the Access Area.

4.2.2. If the Contractor is deemed to be in default under Section 2.2 of these provisions as a result of a failure to pay amount(s) owing by the Contractor, Canada has the right, to be exercised by written notice to the Contractor, to: (i) immediately suspend the right to use the Access Area granted under these provisions (until the failure is remedied by the Contractor); (ii) terminate the right to use the Access Area upon 5 days written notice to cure the default; or (iii) deduct the amount owing from its next payment to the Contractor under the Contract.

4.2.3. If the Contractor abandons the Access Area or stops continuously and actively using the Access Areas for the Permitted Use for more than 15 consecutive days, Canada will have the immediate right, to be exercised by written notice to the Contractor, to terminate the right to use the Access Area.

4.2.4. Canada may at any time terminate the right to use the Access Area (or any portion of it) as of any date, by written notice (the "**Termination Notice**") to the Contractor at least 60 days before the date of termination where the Crown notifies the Contractor of the effective date of the termination (the "**Termination Date**") and that: (i) Canada intends to commence a construction, demolition or redevelopment of all or any portion of the Property such that, in the opinion of the Crown, acting

reasonably, the occupation of the Equipment Area by the Contractor will prevent, obstruct, delay, or otherwise adversely affect that construction, demolition or redevelopment; (ii) Canada has entered into an agreement with another party to occupy office, industrial, retail or residential premises in the Property, and that party requires use of all or a portion of the Access Area; or (iii) Canada has entered into a sale of a portion or all of the Property that includes any portion of the Access Area with a purchaser. In any of these situations, Canada's termination of the Contractor's right to use the Access Area will release the Contractor from its obligations to provide the telecommunications services that required the right to use the Access Area (or the portion of it) to which the Contractor no longer has access.

4.2.5. If: (i) any portion of the Access Area or the Property is damaged or destroyed and cannot be repaired and rendered fit for normal use within 60 days of the happening of the injury; or (ii) any portion of the Access Area or the Property is damaged or destroyed by a cause for which Canada is not insured or not required to insure against or the cost of repairing such damage or destruction exceeds the insurance proceeds available, Canada by giving written notice within 30 days of the injury occurring, may terminate the right to use the Access Area and the Contractor must immediately deliver vacant possession of the Access Area to Canada. In any of these situations, Canada's termination of the Contractor's right to use the Access Area will release the Contractor from its obligations to provide the telecommunications services that required the right to use the Access Area (or the portion of it) to which the Contractor no longer has access.

5. RELOCATION

5.1. Relocation

Canada has the right at any time, by giving no less than 60 days' written notice (the "**Notice of Relocation**"), to relocate the Contractor's Communications Equipment and/or Connecting Equipment to other premises in the Property (the "**Relocated Equipment Area**") in a location determined by Canada in consultation with the Contractor, and the following terms and conditions of this Section 5.1 will apply:

5.1.1. The Relocated Equipment Area accommodating the Communications Equipment must contain approximately the same area as, or greater area than, the Equipment Area, and the Relocated Equipment Area must, in the reasonable opinion of Canada, be suitable for the Contractor's requirements of the Permitted Use.

5.1.2. The Contractor and Canada must share equally in the reasonable, direct, out-of-pocket costs, if any, of moving the Contractor's Equipment and any other Contractor's material contained in the Equipment Area, from the Equipment Area to the Relocated Equipment Area.

5.1.3. The terms and conditions of these provisions apply, mutatis mutandis, to the Relocated Equipment Area, except to the extent that they are inconsistent with the terms and conditions of this Section 5.1.

6. GENERAL

6.1. Rules and Regulations

The use of the Equipment Area under these provisions and access to them is subject to the rules and regulations (as amended from time to time), which Canada may establish from time to time.

6.2. Schedules

Schedules A and B form part of and are included in these provisions.

Schedule A to Annex ___
Communications Equipment; Listing and Specifications
Connecting Equipment; Listing and Specifications

[*to be completed after contract award, if applicable*]

Schedule B to Annex ___
Equipment Area; Floor Plan

[*to be completed after contract award, if applicable*]

ANNEX E - BILLING FORMAT FILE

Contract Total Layout (Record Type-1)

FIELD LOCATION	FIELD NAME	Field Size - Format	DESCRIPTION - EDITS
1	Record Type	1 Numeric - Integer	Record Type = <<1 >>
2 - 9	Invoice Date	8 Numeric - Date	Date invoice is issued YYYYMMDD.
10 - 29	Contract Number	20 Character	Unique Contract Number – Left Justified. Format - "XXXXX-YYCCCC/SSS/UU", or Format - "XXXXXYYCCCC"
30 - 35	Invoice Period	6 Numeric - Date	The year and month that the invoice(s) is being issued for - YYYYMM. This will be used to validate the Invoice Date on the "Type-2" records. (Must be the same)
36 - 65	Contractor's Name	30 Character	Contractor's name - Left Justified.
66 - 77	Total Monthly Charges	12 Numeric-Currency	Total Amount of Charges accumulated from all invoices issued for the month - (Signed with implied 2 decimal) Right Justified.
78 - 89	Total SC+OC&C Amount	12 Numeric-Currency	Total Amount for Service Credits plus Other Charges and Credits for the period - (Signed with implied 2 decimal) Right Justified.
90 - 101	Total HST and/or QST Amount	12 Numeric - Currency	Total Amount Charged for HST and/or QST based on charges for the period - (Signed with implied 2 decimal) Right Justified.
102 - 113	Total GST Amount	12 Numeric - Currency	Total Amount Charged for GST based on charges for the period - (Signed with implied 2 decimal) Right Justified.
114 - 125	Total Late Payment Amount	12 Numeric - Currency	Total Amount charged due to late payment for the period - (Signed with implied 2 decimal) Right Justified.
126 - 137	Total Amount	12 Numeric - Currency	Total Amount Payable according to the Contractors Invoice for the period - (Signed with implied 2 decimal) Right Justified.

Invoice Record by Billing Account Number layout (Record Type-2)

FIELD LOCATION	FIELD NAME	FIELD SIZE - FORMAT	DESCRIPTION - EDITS
1	Record Type	1 Numeric - Integer	Record Type = <<2 >>
2 - 9	Invoice Date	8 Numeric -Date	Date invoice is issued YYYYMMDD
10 - 19	Invoice Number	10 Character	The Invoice Number as submitted by the Contractor
20 - 39	Contract Number	20 Character	Unique Contract Number – Left Justified. Format - "XXXXX-YYCCCC/SSS/UU", or Format - "XXXXXYYCCCC"
40 - 49	BAN	10 Character	Billing Account Number
50 - 55	Invoice Period	6 Numeric -Date	The year and month that the invoice is being issued for - YYYYMM This will be used to validate the invoice date and to validate the Period of Service on the "Type-3" records.
56 - 85	Contractor's Name	30 Character	Contractor's name - Left Justified
86 - 97	Total Monthly Charges	12 Numeric - Currency	Total Amounts (Recurring Amount + Non-Recurring Amount) from all related type 3 records - (Signed with implied 2 decimal) Right Justified
98 - 109	Total SC+OC&C Amount	12 Numeric - Currency	Total Amounts for Service Credits plus Other Charges and Credits (Amount of Service Credits + OC&C by Service/Circuit) from all related type 3 records - (Signed with implied 2 decimal) Right Justified
110-121	Total HST and/or QST Amount	12 Numeric - Currency	Total Amount Charged for HST and/or QST (Accumulated based on all related charges for the invoice) – (Signed with implied 2 decimal) Right Justified
122-133	Total GST Amount	12 Numeric - Currency	Total Amount Charged for GST (Accumulated based on all related charges for the invoice) - (Signed with implied 2 decimal) Right Justified
134-145	Total Late Payment Amount	12 Numeric - Currency	Total Amount charged due to late payment for the period - (Signed with implied 2 decimal) Right Justified
146 - 157	Total Invoice Amount	12 Numeric - Currency	Total Amount Payable According to all Type - 3 and Accumulated from all related charges on the Contractors Invoice - (Signed with implied 2 decimal) Right Justified

Product/Services Record layout (Record Type-3)

FIELD LOCATION	FIELD NAME	FIELD SIZE - FORMAT	DESCRIPTION - EDITS
1	Record Type	1 Numeric - Integer	Record Type = <<3 >>
2 - 9	Invoice Date	8 Numeric - Date	Date invoice is issued YYYYMMDD
10 - 19	Invoice Number	10 Character	The Invoice Number as submitted by the Contractor
20 - 39	Contract Number	20 Character	Unique Contract Number – Left Justified. Format - "XXXXX-YYCCCC/SSS/UU", or Format - "XXXXXYYCCCC"
40 - 49	BAN	10 Character	Billing Account Number
50 - 84	Product Name	35 Character	Product Name convention as defined by the Contractor. This is a mandatory field that is unique to the Product for which this record is being provided (For example **IIS-INT-10GE-xx-or IIS-DDOS-3Gbps-xx**)
85 - 112	Product Code	28 Characters	Unique Circuit Code, as defined by the Contractor (also known as Supplier ID, to uniquely identify the Circuit item for inventory and financial tracking). This is a mandatory field that is unique to the Circuit for which this record is being provided (For example **XOGFYFR1395**)
113 - 142	Location Address Line1	30 Character	Free Format Line 1
143 - 172	Location Address Line2	30 Character	Free Format Line 2
173 - 202	Location Address Line3	30 Character	Free Format Line 3
203 - 232	Location City	30 Character	City Name
233 - 234	Location Prov.	2 Character	Official abbreviation for the Province
235 - 240	Location Postal Code	6 Character	Official Postal Code (ANANAN)
241 - 246	NPANXX	6 Character	The NPA/NXX of the service location
247 - 254	Order Number	8 Character	The SSC Order Authority Number
255 - 262	Product Billing Effective Date	8 Numeric - Date	Date that the billing from the Contractor became effective for the Circuit YYYYMMDD
263 - 270	Circuit Billing Cancel Date	8 Numeric - Date	Date that the billing from the Contractor was stopped for the Circuit YYYYMMDD
271 - 280	Recurring Amount	10 Numeric - Currency	Circuit Monthly Recurring Price (validated to the Contracts Profile Tables) - (Signed with implied 2 decimal) Right Justified
281 - 290	Non-Recurring Amount	10 Numeric - Currency	Circuit Non-Recurring Item Charge (validated to the Contracts Profile Tables) - (Signed with implied 2 decimal) Right Justified
291 - 300	Amount of Service Credits	10 Numeric - Currency	Total Amount of all Discounts and/or Credits for the Circuit, approved by the SSC Service Manager - (Signed with implied 2 decimal) Right Justified
301 - 310	OC&C by Service/Circuit	10 Numeric - Currency	Total Amount of all other Charges and Credits for the service or circuit, approved by the SSC Service Manager -- (Signed with implied 2 decimal) Right Justified

311 - 320	HST or QST Amount	10 Numeric - Currency	Total Amount of HST or QST calculated based on the related accumulated charges for the month for the service or Circuit - (Signed with implied 2 decimal) Right Justified
321 - 330	GST Amount	10 Numeric - Currency	Total Amount of GST calculated based on the related accumulated charges for the month for the service or Circuit - (Signed with implied 2 decimal) Right Justified
331 - 336	Period of Service	6 Numeric - Date	The year and the month during which the service was provided and is being billed for - YYYYMM

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*.]		
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		

Annex A: Statement of Work

Internet Interconnection Service (IIS)
For Shared Services Canada (SSC)

Date: 04April 2013 Version: D11

TABLE OF CONTENTS

List of Appendices

1 INTRODUCTION

(1) Shared Services Canada (hereinafter referred to as SSC) has a requirement for a diverse Internet Interconnection Services (IIS) that will provide it with the ability to access the Public Internet to support the delivery of programs and services to Canadians by Government Departments and Agencies.

(2) The Requirement consists of three redundant IIS Service Interface Points (SIP) provided by two or three separate Internet Service Providers (ISP) (Herein after referred to as Contractor); see Figure 1, where each SIP will have the capacity and the reliability to be able to handle all the Internet traffic in the event of the failure of the others. Other IIS SIPs may be added as and when requested by SSC.

(3) SSC has currently designed the Government of Canada Network (GC.Net) with special routing arrangements that permit the re-routing of its Internet Protocol (IP) traffic when one or more SIPsfail.

(4) All SIPs are active in normal operation and if one or more fail, the remaining functioning SIPs carry the aggregate IP traffic load seamlessly.

(5) Unless otherwise stated, IP refers to IPv4 and IPv6.

(6) The Contractor must provide SSC with an Internet Interconnection Service (IIS), which includes an Anti-Distributed Denial of Service (Anti-DDoS) Scrubbing Service.

(7) Operational objectives include a very reliable IIS with minimum service down time, and a short time to repair.

(8) The IIS services will be managed and operated by two or three separate Contractors; hence some inter-working between Contractors will be required to provide a transparent, efficient and reliable service management and operation.

(9) The Contractor acknowledges that the use of a Contractor provided and Contractor managed Web portal is SSC's preferred method to electronically exchange management and administrative information such as trouble tickets, reports, orders and billing and others. However, other methods such as the use of email, file transfer or others may be considered as alternative methods as well but will require the approval of SSC following Contract Award. This Approved method, tools or Web Portal will be referred to as the Electronics Information Exchange Tool (EIET), further defined in section 8.1.

(10) SSC will identify the persons with the delegated authority for specific roles and responsibilities to the Contractor.

(11) The Contractor must provide the IIS services to SSC on an as and when requested basis, in full compliance with all the requirements of the SOW and in accordance with Annex B-IIS Pricing.

2 INTERNET INTERCONNECTION SERVICE (IIS) REQUIREMENTS

(12) When ordered, the Contractor must provide an IIS service to the Government of Canada Network (GC.Net) to achieve a high availability and a diverse public-facing presence on the Internet. See Figure 1.

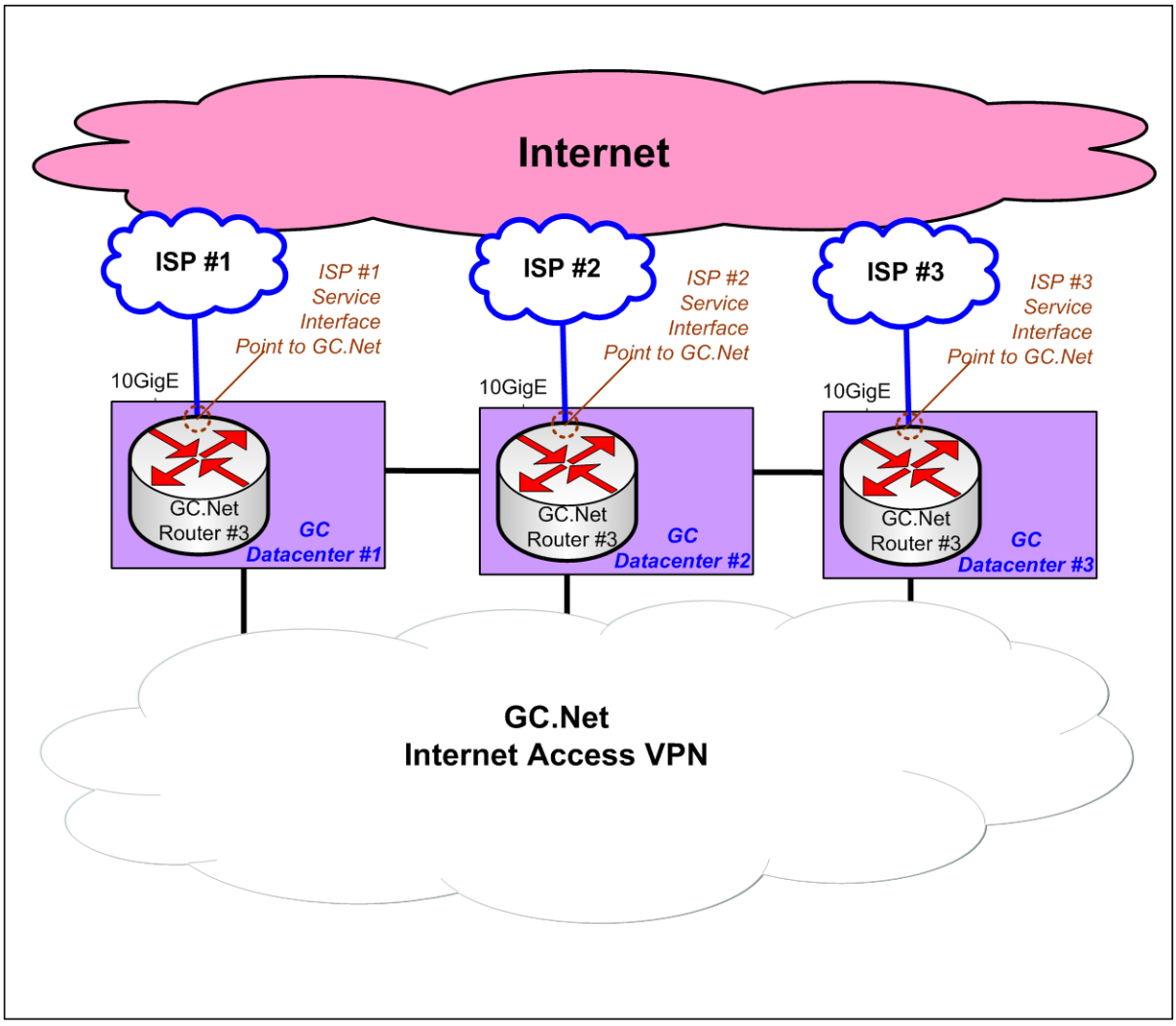

Figure 1: GC.NET Internet Infrastructure

2.1 Infrastructure and Topology

(13) A Service Interface Point (SIP) is the Contractor's demarcation point, interconnecting their IIS to the GC.Net router. The IIS SIP from the Contractor is illustrated in Figure 1.

(14) The SIP transports Internet Protocol version 4 and version 6 (IPv4 and IPv6) datagrams along with all associated route distribution services between the GC.Net and the Internet, according to RFC 4213. Unless otherwise stated, general references to Internet Protocol (IP) will refer to both IPv4 and IPv6.

(15) The IIS SIPs are required to be delivered upon SSC's request to GC Datacenters, two SIPs in the National Capital Region (NCR) and one in the Toronto Region.

(16) The Contractor must also be able to provide additional IIS SIPs within the same GC Datacenter or to other GC Datacenters within the respective NCR and Toronto region when requested.

(17) When requested by SSC, the Contractor must be able to relocate the IIS SIP within the same GC Datacenter or to other GC Datacenters within the same respective region.

(18) The Contractor must provide all networking infrastructure and equipment to connect its SIP to the GC.Net Interconnect Router through a 10 Gigabit Ethernet fibre interface.

(19) The initial committed throughput must be 4 Gigabits per second (Gbps).

(20) The committed throughput will consist of any combination of IPv4 and IPv6 traffic.

(21) The Contractor's IIS must support changes to the committed throughput in increments of 1 Gbps, starting at 4 Gbps, without any service interruption, up to 10 Gbps.

(22) The Contractor's service must be capable of carrying the initial and beyond access subscription throughput (i.e. 4 Gbps and above) through the ISP's network and to the Contractor's Internet peers, on demand.

(23) The Contractor must implement ICMPv6 filtering recommendations as per Request For Comment (RFC) 4890, where the Contractor's network carries IPv6 traffic.

(24) Network Access Point (NAP) interface is the Contractor's router interface that interconnects the Contractor's network to another Internet peer. See Figure 2.

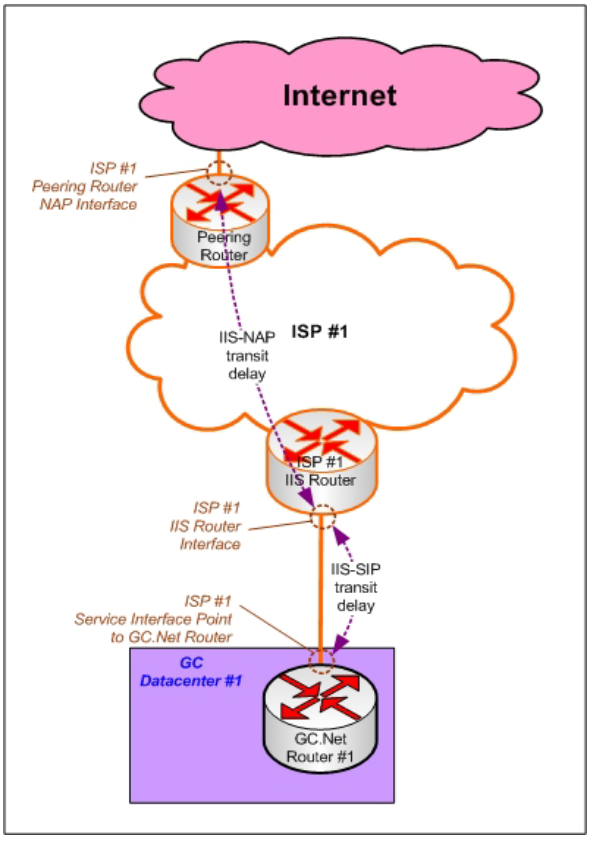

Figure 2 IIS-NAP transit delay and IIS-SIP transit delay

(25) The Contractor's IIS must be capable of carrying at the time of initial installation, 4 Gbps of IP traffic load between the SIP and the Contractor's NAPs.

(26) Within 30 Federal Government Working Days (FGWD) after Contract Award, the Contractor must provide SSC with the capacity engineering plan and design documentation to demonstrate that its current engineered infrastructure and service has the capacity to guarantee this bandwidth.

(27) Throughout the life of the Contract, as the Internet access requirements grow, the Contractor must update SSC, when requested, with its most recent capacity engineering plan and design documentation showing its capacity to transmit the growing Internet traffic while continually meeting the SOW requirements.

(28) The Contractor must connect to two or more Canadian Internet Exchange Points with both IPv4 and IPv6 connectivity.

(29) The Contractor must provide SSC with its service peering and multi-homing arrangements and geographic locations of NAPs.

(30) The Contractor must inform SSC at least 20 FGWDs in advance of any changes made to these arrangements and location details.

(31) The Contractor must notify SSC within 2 FGWDs of any changes to the ownership or leasing agreements of its infrastructure.

(32) The Contractor's physical network infrastructures, connection paths and equipment must be separate and distinct in order to achieve fault tolerant, scalable, and diverse access to the Internet, in support of the interconnect requirements provisioned by redundant interconnections.

(33) If a single Contractor provides more than one SIP, the connection paths and equipment including the Anti-DDoS systems for each SIP must be separate unless otherwise approved by SSC.

(34) To resolve interconnection or performance issues, or to replace no-longer-supported components, SSC may from time to time upgrade its border router. SSC will notify the respective Contractor of any upcoming upgrades at least 30 FGWDs in advance.

(35) The Contractor must maintain its interfacing and infrastructure equipment, to meet the service levels, specified in the Service Level Management section.

(36) The Contractor must ensure that the IP traffic is not shaped in this service.

(37) Upon request, the Contractor must demonstrate that the service is providing the required throughput.

(38) The Contractor must provide any test equipment required to perform the demonstration.

2.2 Border Gateway Protocol (BGP)

(39) The GC.Net is not a transit Autonomous System (AS) for other Internet Service Providers, or for networks other than those belonging to the GC.Net.

(40) The GC.Net treats a downstream network as either a stub AS or as part of GC.Net itself (i.e. AS 2669). See Figure 3.

(41) The GC.Net performs its own route aggregation, and maintains its own routing registry information at Routing Arbiter Database (RADB), which the Contractor must use in the creation of applicable prefix filters.

(42) IP traffic between GC.Net clients will not be routed outside of the GC.Net.

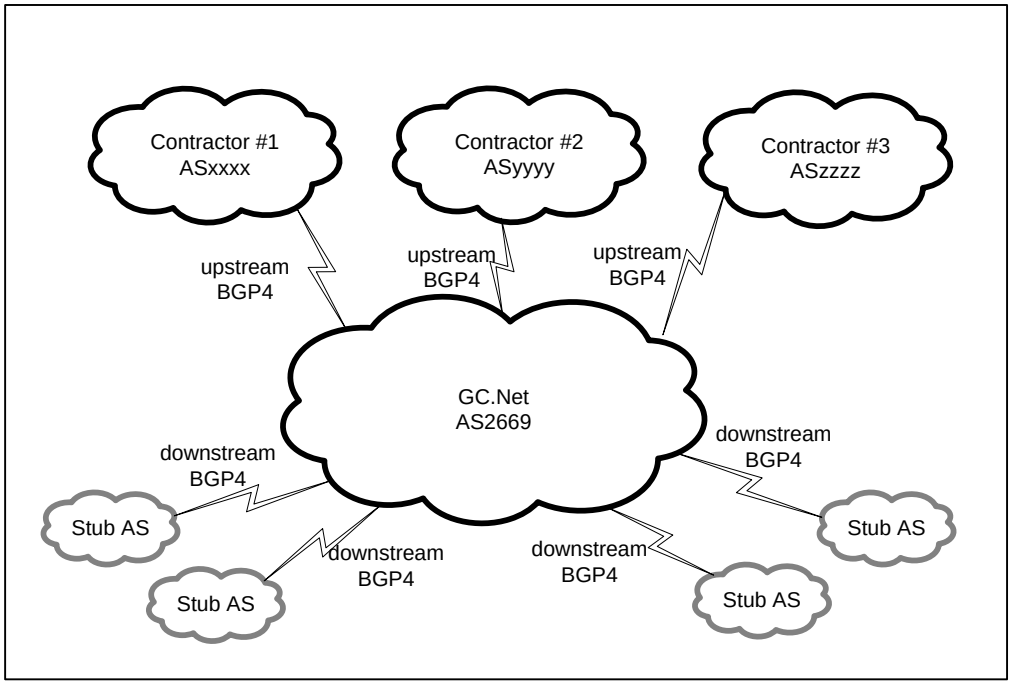

Figure 3: GC.Net Autonomous Systems

(43) The Contractor's IIS must accept upstream IP traffic along with routing information from the SIP.

(44) The Contractor must support BGP version 4 as per RFC 4271.

(45) The Contractor must implement the multi-homing BGP design used by the GC.Net to direct IP traffic to and from the Internet.

(46) The Contractor may request deviations from this design or propose an alternative design, subject to SSC's approval.

(47) The Contractor must provide an external BGP4 connection to the GC.Net and must have a different and unique AS number.

(48) The Contractor must implement and support BGP features as documented by the Internet Engineering Task Force (IETF) by Request for Comments (RFC) 1772 through 1774, RFC 4760, RFC 4893 and RFC 4273, including but not limited to the following:

(48.a) Support all mandatory BGP functions and well-known attributes;

(48.b) Support all transitive BGP attributes (i.e. pass-thru to other AS without modification);

(48.c) Support MD5 Signature Option to protect the BGP from session resets and malicious data injection;

(48.d) Support Multi-Protocol BGP (RFC 4760); and

(48.e) Support 32-bit ASNs

(49) The Contractor's IIS must accept BGP4 route announcements from the GC.Net ASN.

(50) The Contractor's IIS must not filter, reject or block route advertisements provided by the GC.Net on any criterion other than the following:

(50.a) Implement IETF BCP 38;

(50.b) Any IPv4 route advertisement with a mask element longer than 24 bits; and

(50.c) Any IPv6 route advertisement with a mask element longer than 48 Bits.

(51) The Contractor must not modify GC.Net routing information without prior written consent from SSC.

(52) The Contractor must not aggregate GC.Net address space beyond the level of aggregation provided by GC.Net route advertisements.

(53) The Contractor's IIS must accept route object information from the GC.Net in Routing Policy Specification Language (RPSL) object format, as specified in RFC 2622 and RFC 4012.

(54) The Contractor must not implement route flap dampening according to recommendations in RIPE BCP 378.

(55) The Contractor's IIS must not accept Network Announcement Change Requests (NACR), unformatted mail messages, or others in similar format or mechanisms. The Contractor must send an e-mail notification to SSC within 1 FGWD of receipt of request of changes to the routing information, and within 2 FGWDs after implementing the requested changes to the routing information.

(56) The Contractor must provide a method by which SSC may signal to the Contractor's network by use of a Contractor supplied BGP community, to remotely trigger a black hole (RTBH) of any Internet or GC.Net route as a defensive counter measure in the case of a network based attack on any portion of the GC.Net as illustrated in RFC 3882 and RFC 5635.

2.3 Service Interface Point (SIP) Configuration

(57) The IIS SIP must be configured for full-duplex auto sensing mode.

(58) The Contractor will supply from their address resources a static /30 IPv4 address and a static /126 IPv6 address for interconnection between the GC.Net border router and the Contractor's border router and disable any IPv6 stateless auto-configuration, DHCP and DHCPv6 protocols on their interface. No Ipv6 site-local addresses shall be used. Ethernet frames forwarded on the interface shall have the following ethertypes: 0x0800 (IPv4), 0x0806 (ARP) and 0x86dd (IPv6).

(59) The Contractor's service must support IP traffic for link-local protocols such as but not limited to IRDP, ICMP redirects, interior-routing protocol broadcasts (OSPF, IS-IS, IGRP, EIGRP), vendor-proprietary discovery protocols (such as CDP and EDP), BOOTP, MPD, LLDP and IEEE 802.1D shall not be forwarded except for ARP, MLDv2 (RFC 3810), IGMPv2 (RFC 2236) 7 v3 (RFC 3376) and IPv6 Neighbour Discovery (RFC 4861).

2.4 Support for IPv4 and IPv6 Multi-Cast

(60) For IPv4 multi-cast, the Contractor must:

(60.a) Establish a PIM (RFC 4601) version 2 sparse mode connection with the GC border router;

(60.b) Apply a PIM boundary on the vendor router interface to define their own PIM domains separate from the PG PIM domain;

(60.c) Establish a MSDP peer with the IPv4 address supplied to the GC border router that filters unwanted multicast addresses in egress and ingress directions according to the best current practices and accepts (S, G) source pairs from the GC border router.

(61) For IPv6, the Contractor must activate PIM v2 aparse mode on their router's interface.

(62) For the interface connecting the GC border router and the Contractor's router:

(62.a) For IPv4 multi-cast, IGMP version 2 or above (RFC 3376) must be enabled on the interface;

(62.b) For IPv6 multi-cast, MLDv2 (RFC 3810) must be enabled on the interface.

(63) The Contractor must not filter PIM source-specific multi-cast (RFC 3659 and RFC 4608) for either IPv4 multi-cast or IPv6 multi-cast.

(64) The Contractor must not activate PIM dense mode (RFC 3973) on the interface connecting to the GC border router.

2.5 Additional Bandwidth Required under Special Situations

(65) The Contractor must always support additional IP traffic within the committed throughput, including sudden large increases compared to recorded levels from the previous month. In the event of a catastrophic failure of the planned interconnection configuration, whereby all rather than just a portion of the IP traffic will be flowing to and from the Internet, will be rerouted automatically through the Contractor's IIS.

(66) The Contractor must provide for additional throughput to accommodate IP traffic bursts and allow for ongoing growth without constraining demand and ensure Internet service availability, as the Contractor will not be notified in advance of such situations.

(67) The Contractor is not allowed to use Zero Committed Information Rate (CIR) or Unspecified Bit Rate (UBR) circuits.

(68) The Contractor must provide committed throughput.

(69) The Contractor may use circuits configured by sustained cell rates, committed information rates, committed access rates or similar schemes for guaranteed bandwidth.

(70) The Contractor's IIS must use full duplex operation.

2.6 Anti-Distributed Denial of Service Scrubbing Service

(71) When ordered, the Contractor must provide Anti-Distributed Denial of Service (Anti-DDOS) Scrubbing Service within the Contractor's infrastructure.

(72) The Contractor must provide the ability to analyze the IP traffic to and from the Internet, and detect and remove (i.e. scrub) malicious IP traffic based upon signatures, reputation and IP traffic anomalies. The Contractor must provide the capability for SSC to obtain and export meta data and logs associated with a real or suspected cyber attack.

(73) The Contractor must provide the ability to allow legitimate IP traffic traverse to its destination and prevent any Denial of Service attacks overwhelming the IIS SIP.

(74) The Contractor must provide access and be able to configure the respective Contractor's Anti-DDOS service via the EIET

(75) The Contractor must provide SSC with a secure access to the EIET.

(76) The Contractor must allow SSC to perform the following activities on the EIET:

(76.a) Execute, view and download reports.

(76.b) Configure and define reports on Anti-DDOS as required.

(76.c) Enable mitigation or disable mitigation against a DDOS event.

(77) The Contractor must send near-real time alerts to SSC either through email or text message based on configured key trigger or intrusion events.

(78) The Contractor must send an email or text message at the start and stop of each event. The message must include information on the type of event, service affected, severity level, time started, time ended, source(s) of attack, destination(s) of attack, and description of effects.

(79) The Contractor must provide real-time reporting of DDOS IP traffic data on the EIET .

(80) The Contractor must store 5-minute aggregate IP traffic data for the previous 14 days and this data must be available for query on the EIET.

(81) The Contractor must store 30-minute aggregate IP traffic data for the previous 8 weeks and this data must be available for query on EIET.

(82) The Contractor must store 2-hour aggregate IP traffic data for the previous 6 months and this data must be available for query on the EIET.

(83) The Contractor must store 1-day aggregate IP traffic data for the previous 3 years and this data must be available for query on the EIET.

(84) The Contractor must be proactive through continual monitoring for cyber threats from Denial of Service attacks and provide notifications followed up by mitigation recommendations to SSC when and if the Contractor is made aware of cyber threats targeting SSC, that may potentially impact the Government of Canada Network and implement the mitigations, once approved by SSC.

(85) The Contractor must provide Anti-DDOS systems with initial protection capacity of 2Gbps of Internet Bandwidth, with the option to increase this capacity upon request in 1Gbps steps.

(86) The Contractor must be able to mitigate up to five (5) ongoing attack streams, including black hole mitigations, with the option to increase this number, based on demand.

(87) The Contractor must support one (1) configuration with a bandwidth profile that can be globally applied to all traffic at the IIS pipe level and multiple configurations and bandwidth profiles for the individual networks running on this pipe.

(88) The Contractor must provide Anti- DDOS system that is capable of learning the normal traffic patterns for all profiles for specific normalization durations of at least 60 days and set normal bandwidth thresholds accordingly.

(89) The Contractor must provide recommendations for the initial system configuration and thresholds for the initial set-up as a baseline, as well as when updates are required for the duration of the Contract, as applied and approved by SSC.

(90) The Contractor must provide these recommended updates within 72 hours as part of the post-incident report, when a DDOS Incident is not completely mitigated by the current service being provided and modifications are required to the system configuration and thresholds. The Contractor must demonstrate that these recommendations are in the best interest of SSC.

(91) The Contractor must react to the demands of SSC in the case where SSC advises the Contractor of an eminent cyber threat. Once identified, the Contractor must take immediate action, as per Incident Management Section 5.4, to implement recommendations to provide protection against cyber threats, through system

configuration and threshold changes, which will then be documented in post incident reports, for protection and due diligence against potential future cyber threat scenarios.

(92) The Contractor must provide a point of contact (PoC) to SSC to answer questions and discuss cyber threats and recommendations for mitigation of a security incident.

3 OPERATIONAL READINESS

3.1 Operational Readiness Plan

(93) The Contractor must submit an Operational Readiness Plan (ORP) for approval to SSC within 15 Federal Government Work Days (FGWD) of Contract award that identifies a schedule to become operationally ready after Contract award.

(94) The Contractor must provide a revised ORP within 5 FGWDs of receiving comments from SSC on the ORP.

(95) Unless indicated otherwise herein, the Contractor must complete the following Work (further detailed in sections 3.2 through 3.5) within 30 FGWDs following acceptance of the ORP, excluding days required by SSC for review and approval of the Work:

a) Service Management Plan;

b) Service Continuity Plan;

c) Service Design; and

d) Service Description.

(96) The Contractor must provide a weekly operational readiness progress report to SSC which will identify for each task/milestone/deliverable in the ORP the following information:

a) Current status;

b) Expected completion date; and

c) Summary of work activities for the next reporting week.

(97) SSC will organize and conduct a Contract launch meeting within 10 FGWDs of Contract award. The agenda for the meeting will be defined by SSC, which will be provided to the Contractor prior to the Contract launch meeting.

3.2 Service Management Plan

(98) The Contractor must provide a Service Management Plan to SSC which includes:

(98.a) Executive summary description of the IIS;

(98.b) Resource Plan that includes a methodology for determining resource levels required to complete the Work under the Contract.

(98.c) Quality Assurance plan that includes an approach to formulating and enforcing work and quality standards, ensuring compliance with Service Levels, and reviewing work in progress;

(98.d) Communication Plan that includes an approach for communicating individual task requirements, resolving issues and risks between the Contractor and SSC, and managing communications between the Contractor and SSC;

(98.e) Organizational Plan that includes management structure, organizations, and roles and responsibilities of key personnel and subject matter experts;

(98.f) Risk Management Plan that includes the approach for identifying and tracking risks, isolating the event triggers for risks, assessing probability and impact, as well as identifying a mitigation plan;

(98.g) Issue Management Plan that includes the approach for identifying and managing service management issues, isolating the issues, assessing the impacts, identifying responsible parties, assessment of a severity and priorities, and processes for determining a resolution; and

(98.h) Information Systems Overview that includes a description of information systems implemented for the IIS.

3.3 Service Continuity Plan

(99) The Contractor must provide a Service Continuity Plan to SSC for disaster recovery and business resumption of the IIS that includes:

a) A strategy for restoring the service;

b) Processes that will be used to effect service continuity (for example, communications strategy, service restoration prioritization);

c) Transferring operational and management functionality in the primary operations centre to the backup operations centre;

d) Back up strategies for facilities, operational support systems and data, and key service components;

e) Ensuring that its suppliers (if applicable) have in place disaster recovery plans and strategies; and

f) Timeframes that SSC can expect services to be restored.

3.4 Service Design

(100) The Contractor must provide a Service Design to SSC for the IIS that includes:

a) The design methodology;

b) A network security architecture blue print of the service being offered, that describes the implementation of security perimeter safeguards, the placement of services in network security zones and the redundancy, scalability and security features to support the Service Levels;

c) The content and format of reports and documentation; and

d) The manufacturer specifications of all equipment that will be deployed to provide the IIS service.

3.5 Service Description

(101) The Contractor must provide a Service Description to SSC for the IIS that includes**:**

a) An overview of the IIS;

b) Service Level measurement processes;

c) An overview of service reports to be provided;

d) Management service processes (change, incident, problem, configuration, release, availability and capacity management);

e) Service Desk processes; and

f) Operations Centre processes.

3.6 Security Assessment and Authorization (SA&A)

(102) The Contractor must perform the Work in this subsection as part of SSC's security assessment and authorization process for the IIS.

(103) The SA&A process must be completed before the actual implementation of IIS.

(104) The Contractor must meet Security Assessment and Authorization requirements for IIS, consisting of a three gate process specified as follows:

a) Gate 1 - High-Level Service Design:
   i) High-Level Service Design Security Specification,
   ii) Security Requirements Traceability Matrix (SRTM);

b) Gate 2 - Detailed Service Design:
   i) Detail Design Security Specification;
   ii) Security Requirements Traceability Matrix;
   iii) Change Management;
   iv) Protection of Development Environment;
   v) Secure Development Practices;
   vi) Operational Security Procedures, and
   vii) Security Installation Procedures.

c) Gate 3 - Installation:
   i) Integration Security Test Plan and Test Report;
   ii) Vulnerability Assessment and Mitigation Plan and Report;
   iii) Security Installation Verification Plan and Report;

3.6.1 Gate 1 – SA&A High-Level Service Design

(105) The Contractor must provide SSC with a draft version of the following deliverables within 30 Federal Government Working Days after Contract award for approval by SSC:

a) high-level service design security specification (see High-Level Service Design Security Specification subsection), and

b) security requirements traceability matrix (see Security Requirements Traceability Matrix subsection).

(106) SSC will review the draft deliverables within 5 Federal Government Working Days.

(107) The Contractor must provide SSC with updated deliverables according to feedback received from SSC within 5 Federal Government Working Days after receiving the feedback.

(108) SSC will review the final deliverables within 5 Federal Government Working Days.

(109) The Contractor must provide SSC with final deliverables according to feedback received from SSC within 2 Federal Government Working Days after receiving the feedback.

(110) The Contractor must wait for Gate 1 approval by SSC before proceeding with the next gate of the security assessment and authorization.

3.6.1.1 High-Level Service Design Security Specification

(111) The Contractor must provide SSC with a high-level service design security specification document that describes the high-level security design aspects of the IIS. At a minimum, the high-level service design security specification must contain the following information:

a) a high-level component diagram that clearly shows the allocation of services and components to network security zones and identifies key security related data flows;

b) a description of the network zone perimeter defences;

c) a description of the use of virtualization technologies, where applicable;

d) descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers;

e) descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements;

f) a description of the approach for remote management;

g) a description of the approach for access control;

h) a description of the approach for security management and audit;

i) a description of the approach for configuration management;

j) a description of the approach for patch management; and

k) justification for key design decisions.

(112) The high-level service design security specification must describe how the following concepts will be implemented:

a) access control;

b) security management and audit;

c) configuration management;

d) patch management; and

e) remote management.

(113) The high-level service design security specification must describe the allocation of the security requirements at each of the architecture layers of the high-level service design.

(114) The high-level service design security specification must define the architectural layers (e.g., communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer).

(115) The high-level service design security specification must explicitly document justification for key security design decisions as they relate to:

a) network security zoning;

b) network and network zone perimeter defence; and

c) use of virtualization technology.

(116) The high-level service design security specification must be compliant with the service design (see Service Design subsection).

3.6.1.2 Security Requirements Traceability Matrix

(117) The Contractor must provide SSC with a security requirements traceability matrix (SRTM) that provides for the security requirements of IIS including documentation references within the service high-level service design security specification that describe the security safeguards to be implemented. The SRTM must provide assurance that the IIS high-level service design security specification fully satisfies its security requirements for IIS.

(118) All service documentation referenced in the STRM must be provided to SSC with the SRTM and must describe the security safeguards in sufficient detail to allow SSC to confirm that the security safeguards satisfy the security requirements of the IIS.

(119) At a minimum, the SRTM must contain, for each security requirement, the following information:

(120) the security requirement identifier (SEC ID) that maps the security requirement to the corresponding statement in the SOW (e.g., heading or line ID);and

(121) tracing (a reference to an identifiable element) to high-level service design specifications.

3.6.2 Gate 2 – SA&A Detailed Service Design

(122) The Contractor must provide SSC with a draft version of the following deliverables within 50 Federal Government Working Days after Contract award for approval by SSC a detailed service design security specification (see Detail Design Security Specification subsection),

(123) The Contractor must provide an updated security requirement traceability matrix traced to detailed service design (see Security Requirements Traceability Matrix Traced To Detailed Service Design subsection).

(124) SSC will review the draft deliverables within 5 Federal Government Working Days.

(125) The Contractor must provide SSC with updated deliverables according to feedback received from SSC within 5 Federal Government Working Days after receiving the feedback.

(126) SSC will review the final deliverables within 5 Federal Government Working Days.

(127) The Contractor must provide SSC with final deliverables according to feedback received from SSC within 2 Federal Government Working Days after receiving the feedback.

(128) The Contractor must wait for Gate 2 approval by SSC before proceeding with the next gate of the security assessment and authorization.

3.6.2.1 Detailed Service Design Security Specification

(129) The Contractor must provide SSC with a detailed service design security specification document that describes the detailed security design aspects of the IIS. At a minimum, the Detailed Service Design Security Specification must contain the following information:

a) a detailed component diagram (this should be a refinement of the high-level component diagram);

b) descriptions of the allocation of technical security mechanisms to detailed service design elements;

c) descriptions of the allocation of non-technical security mechanisms to high-level organizational or operational elements; and

d) justification for key design decisions.

(130) The detailed service design security specification must be compliant with the service design (see Service Design subsection) and the high-level service design security specification (see High-Level Service Design Security Specification subsection).

3.6.2.2 Security Requirements Traceability Matrix Traced To Detailed Service Design

(131) The Contractor must provide SSC with an updated security requirements traceability matrix (SRTM) that provides for the security requirements of the IIS that includes the documentation references within the service detailed service design security specification that describe the security safeguards to be implemented. The SRTM must provide assurance that the IIS high-level service design security specification fully satisfies its security requirements.

(132) All service documentation referenced in the SRTM must be provided to SSC with the SRTM and must describe the security safeguards in sufficient detail to allow SSC to confirm that the security safeguards satisfy the security requirements of IIS by SSC.

(133) At a minimum, the SRTM must contain, for each security requirement, the following information:

a) the security requirement identifier (SEC ID) that maps the security requirement to the corresponding statement in the SOW (e.g., heading or line ID);

b) tracing (a reference to an identifiable element) to high-level service design specifications, and

c) tracing (a reference to an identifiable element) to detailed service design specifications.

3.6.3 Gate 3 – Installation

3.6.3.1 Integration Security Test Plan and Test Report

(134) The Contractor must provide Security Testing Plan to SSC that documents the test cases.

(135) The Contractor must implement the Security Testing Plan and provide SSC with a Security Testing Report that includes:

a) The Security Testing procedure to confirm that the security safeguard is implemented correctly and satisfies applicable standards as specified in the service design specifications;

b) The expected and actual results for each Security Testing procedure;

c) For each deviation from the expected result, that could be corrected at the time of verification, a description of the corrective measure(s) that were implemented in the IIS; and

d) For each deviation from the expected result that could not be corrected at the time of verification (e.g., due to more significant changes), include the deviation in the

Risk Treatment Plan.

(136) The Contractor must allow SSC to witness the Security Testing that includes:

a) Physical access to the Contractor's facilities where the implementation of the IIS is located; and

b) Ability to observe Contractor representatives while they execute the Security Testing procedures.

3.6.3.2 Vulnerability Assessment and Mitigation Plan and Report

(137) The Contractor must allow SSC to conduct a Vulnerability Assessment against the IIS that includes:

a) Physical access to the Contractor's facilities where the IIS infrastructure (hardware and software components) are located;

b) Network access(es) to the IIS to allow for the scanning of network and host devices; and

c) Assistance for the duration of any onsite portion of the Vulnerability Assessment of at least one technical resource that is familiar with the technical aspects of the IIS (i.e., the hardware, software, and network products and their configuration).

(138) SSC may conduct a Vulnerability Assessment against the IIS and provide a Vulnerability Assessment report to the Contractor that will identify the vulnerabilities that were detected by SSC.

(139) SSC will limit its Vulnerability Assessment to discovery and scanning activities and will not engage in disruptive or destructive activities.

(140) SSC at its discretion may request that the Contractor perform the Vulnerability Assessment testing using a plan approved by SSC and provide the result of the testing to SSC.

(141) The Contractor must provide SSC with a Vulnerability Mitigation Report that includes:

a) A list of vulnerabilities for which SSC is recommending the implementation of corrective measures;

b) A description of the corrective measure to be implemented including expected timeframes; and

c) Updates to all documentation affected by the corrective measures implemented including documentation referenced in the SRTM.

(142) The Contractor must complete the Work for Vulnerability Assessment and Vulnerability Mitigation report, according to a plan approved by SSC.

3.6.3.3 Security Installation Verification Plan and Report

(143) The Contractor must provide SSC with a Security Verification Test Plan that documents the test cases.

(144) The Contractor must implement the Security Verification Test Plan and provide SSC with a Security Verification Report.

(145) The Security Verification Report will identify that:

a) The Security Verification procedure confirms that the security safeguard is implemented correctly and satisfies applicable standards as specified in the service design specifications;

b) The expected and actual results are shown for each Security Verification procedure;

c) For each deviation from the expected result, a description of the corrective measure(s) that were implemented in the IIS for the ones that could be corrected at the time of verification; and

d) For each deviation from the expected result that could not be corrected at the time of verification (e.g., due to more significant changes), the deviation is to be included in the Risk Treatment Plan.

(146) The Contractor must allow SSC to witness the Security Verification testing that includes:

a) Physical access to the Contractor's facilities where the implementation of the IIS is located; and

b) Ability to observe Contractor representatives while they execute the Security Verification procedures.

3.6.4 Security Concept of Operations

(147) The Contractor must provide a Security Concept of Operations Report to SSC that describes the:

a) User community;

b) Contractor applications used for service operation;

c) Contractor data center and communication facilities;

d) Security roles and responsibilities of the Contractor;

e) Incident Analysis and Post Incident Reporting;

f) Access controls; and

g) Contractor's operational environment.

3.6.5 Security Risk Management Plan

(148) The Contractor must provide a Security Risk Management Plan to SSC that includes:

a) How security risks will be reported (to whom and at what frequency);

b) Roles and responsibilities toward security risk management; and

c) How security risks will be tracked and addressed.

3.6.6 Security Architecture

(149) The Contractor must provide a Security Architecture Report to SSC that describes for the Contractor's infrastructure:

a) How Public Access Zone (Public Access Zone is described in CSEC publication ITSG-22 [http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-eng.pdf] and ITSG-38 [http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg38-eng.pdf]) interfaces are strictly controlled, including all external controlled networks such as the Internet, at a defined security perimeter;

b) How other network security zones are established in accordance with the

Communication Security Establishment Canada ITSG-22;

c) How Security Assessment and Authorization is addressed in accordance to ITSG-33 in support of continuous monitoring and mitigation while assessing the performance of common security controls of the information support systems.

d) The equipment used by the Contractor in the provisioning of IIS directly and indirectly interfacing with Government of Canada infrastructure (e.g. Routers) must have previously received validation under a recognized Common Criteria scheme, either against an approved Protection Profile, of if one does not exist, an applicable security target, whose assurance requirements conform either to EAL 2 or an approved assurance package.

e) Cryptographic modules employed in accessing the EIET , shall be validated to the FIPS 140-2 standard or subsequent standards, to encrypt communications between the Government of Canada and the Contractor.

f) The FIPS 140-2 validated cryptographic modules shall be configured to operate in FIPS mode, in order to utilize only CSEC approved algorithms and key sizes. CSEC approved algorithms and key sizes are documented in IT Security Alert 11 Version E, (ITSA-11E) and are subject to change.

g) The Contractor must include a brief overview description of the network diagrams provided.

3.6.7 Security Operational Procedures

(150) The Contractor must provide the Contractor's Security Operational Procedures to SSC that describes the:

a) System hardening requirements applied to servers, data warehouse, network devices, applications and the procedures used to verify the hardening;

b) Functions of the operating environment that include:

i) Power up/power down sequence;

ii) Use of privileged system accounts;

iii) Start up/shut down of systems (including operating system and applications);

iv) Start and stop communications;

v) Backup and restore;

vi) Over-riding of security controls (if applicable); and

vii) Recovery/restart.

c) Incident response priorities and processes to mitigate damage, contain the cause of the incidents and restore services including notification to SSC;

d) Types of event or activities that constitute a security incident, descriptions of the IT security incidents that can occur, their potential impact, the technical and operational environment, and service delivery priorities;

e) Privacy breach protocol including but not limited to breach notification processes; and

f) Processes to monitor for system security vulnerabilities and to apply security patches accordingly.

3.6.8 Security Incident Notification

(151) The Contractor must provide notification and generate Security Incident Tickets that include but not limited to the following information:

a) Type and description of an attack,

b) Whether attack appears to have been successful and impact,

c) Attack scope (to one or many client groups),

d) Suspected source/origin of attack, incident or event

e) actions taken, and

f) Status of mitigation.

3.6.9 Risk Treatment Plan

(152) The Contractor must provide SSC with a Risk Treatment Plan to track and address all outstanding:

a) Risks where security or functional requirements are not being met;

b) Deviations requiring correction identified in Security Verification testing;

c) Deviations requiring correction identified in Security Testing; and

d) Corrective measures identified in the vulnerability mitigation report.

(153) The Risk Treatment Plan must include for each corrective measure:

a) Who is responsible for implementing the corrective measure;

b) What timeframe is targeted for mitigation of the risk (Date/Release);

c) An assessment of residual risk once the corrective measure is implemented; and

d) A priority level, as specified by SSC, for the implementation of each corrective measure.

3.7 Implementation of the IIS

(154) The Contractor must provide and maintain the components for the IIS.

(155) The Contractor must implement the IIS at sites as specified by SSC.

(156) The Contractor must implement the IIS in conformance to the following and as items are updated and amended from time to time:

a) Service Design (refer to Service Design Section);

b) Security Requirements;

c) Security Architecture (refer to Security Architecture section);

d) Security Operational Procedures (refer to Security Operational Procedures section);

e) ITSB 60: Guidance on the Use of the Transport Layer Security Protocol within the Government of Canada (http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb60-

eng.html);

f) ITSB 61: Guidance on the Use of the IP Security Protocol within the Government of Canada (http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb61-eng.html);

g) W3C's Web Content Accessibility Guidelines (WCAG) 2.0 Level AA – guideline 1 and 2 (http://www.w3.org/TR/WCAG20/);

(157) The Contractor must implement the corrective measures identified in Security Verification, Security Testing and Vulnerability Mitigation report according to the Risk Treatment Plan in a priority order specified by SSC.

(158) The Contractor must provide a report within 20 FGWDs of completion of the Risk Treatment Plan that identifies any test results to verify the effectiveness of the corrective measures implemented.

3.7.1 Progress Meetings and Reporting

(159) The Contractor must provide weekly status report to SSC on the progress of the IIS Implementation.

(160) The Contractor must attend meetings as scheduled by SSC to ensure that the work proceeds according to the implementation schedule.

3.7.2 Implementation Milestones

(161) The implementation Plan must include the following three milestones:

(161.a) Preliminary Design,

(161.b) Critical Design, and

(161.c) Operational Readiness Review.

3.7.2.1 Preliminary Design

(162) The Contractor must schedule a site survey with SSC and perform a site survey to locate and assess all information required to install and provide the IIS at the GC data centre.

(163) The details include technical interface between the Contractor's IIS and the GC.Net, and Contractor's requirements for electrical power, space, heating and ventilation.

(164) The Contractor must document the site survey and deliver it to SSC within 2 FGWDs after the site visit.

(165) The Preliminary Design is completed when SSC approves the site survey.

3.7.2.2 Critical Design

(166) The Contractor must provide a draft IIS Configuration Document for review by SSC. The draft must include a copy of the configuration of the Contractor's IIS router (with passwords deleted from the interface).

(167) The Contractor must identify to SSC from the site survey any missing infrastructure or prerequisites that SSC may have to provision in time for upcoming installs.

(168) The Contractor must provide network and service information to demonstrate the Contractor's IIS can meet all performance requirements.

(169) The Contractor must identify if the information provided is considered proprietary.

(170) After the receipt of the IIS Configuration Document, the Contractor must meet with SSC to discuss any issues found in the documents.

(171) Based on the feedback from SSC, the Contractor must issue a final IIS Configuration Document for approval by SSC.

(172) During the life of the Contract, the Contractor must maintain the IIS Configuration Document to ensure it is up-to-date and reflects the actual network configuration for the service.

(173) The Contractor must deliver and obtain approval from SSC for any revisions to the document within 5 FGWDs.

(174) The Contractor must finalize its IIS design, network configuration, equipment and facilities for the provision of the service.

(175) The Contractor must deliver their Operations and Service Management Procedures in this phase to SSC.

(176) The Critical Design is completed when SSC approves the IIS Configuration Document and related activities are completed.

3.7.2.3 Operational Readiness Review

(177) The Contractor must perform sufficient testing prior to providing their services to SSC. The Contractor must record and document all test results and send them to SSC for review and approval.

(178) The Contractor must deliver final versions of the Operations Management Procedures and Service Management Procedures for approval by SSC.

(179) SSC may perform certain tests to validate the correct operation of each Contractor's service and to verify that performance requirements are met.

(180) The Contractor must facilitate and support SSC in the testing. The testing period will be 48 hours after the Contractor designates the service as operational. During this period, SSC may:

(180.a) Use "Ping", "Traceroute" and any other necessary procedures to test network connectivity;

(180.b) Verify that the network numbers to be propagated into the global Internet are correctly propagated;

(180.c) Verify network numbers not to be propagated into the global Internet are not propagated;

(180.d) Verify that non-GC.Net packets do not transit the GC.Net between IIS interfaces; and,

(180.e) Perform any test deemed necessary to validate the IIS performance such as Availability, Throughput, Transit Delay and Packet Loss.

(181) The Operational Readiness Review is completed when SSC approves all reports, EIET, documents and procedures detailed in the Reporting and Documentation Section of the SOW as well as when the IIS passes all acceptance tests and meets the performance requirements.

(182) The successful testing and signoff of the Operational Readiness Review by SSC designates the point in time when the Contractor may start billing for the IIS.

3.7.3 Authentication, Integrity and Confidentiality

(183) The IIS must be transparent to requests to establish a VPN Tunnel using any of the following Authentication Services as specified by SSC:

a) Certificate;

b) Radius Server;

c) LDAP Server;

d) Secure ID Server; and

e) Active Directory.

(184) The IIS must allow Certificates provided by SSC.

3.7.4 Network Connectivity

(185) The Contractor must not firewall or filter application protocol traffic.

4 SERVICE MANAGEMENT

(186) The Contractor must provide a Service Manager who will be SSC's initial point of contact and liaison for, but not limited to:

a) Incident escalation;

b) Root cause analysis (RCA);

c) Service levels;

d) Implementation activities;

e) Maintenance and release window scheduling;

f) Service quality;

g) Service assurance;

h) Service consultation;

i) Service reporting;

j) Service performance and availability; and

k) Service processes.

(187) The Contractor must provide a Service Architect who will be SSC's single point of contact for:

a) Planning, designing and engineering;

b) Analyzing requirements and impacts; and

c) Identifying and recommending changes.

(188) The Service Manager must be available to meet with representatives of SSC during FGWDs from 08:00 to 17:00 ET within 2 FGWDs of a request by SSC.

(189) The Service Architect must be available to meet in person with representatives of SSC during FGWDs from 08:00 to 17:00 ET within 2 FGWDs of a request by SSC.

4.1 Operations Centre

(190) The Contractor must provide a Primary Operations Centre 24 hours per day, 7 days per week, 365 days per year with the infrastructure and resources required for the centralized management and operation of the IIS.

(191) The Contractor must manage and coordinate the boot up and shut down of all components under their responsibility in providing the IIS when requested by SSC, at no additional cost to SSC. This will include periods when Data Centres under the control of SSC must be shut down, which may impact the operation of co-located IIS components.

(192) The Contractor must also provide a Backup Operations Centre, which is not physically located with the Primary Operations Centre (i.e. same building), that provides all operational and management functionality supported by the Primary Operations Centre.

(193) The switchover from the Primary Operations Centre to the Backup Operations Centre must be transparent to SSC and not impact the operations of the IIS.

(194) The Contractor must switchover from the Primary Operations Centre to the Backup Operations Centre according to the Service Continuity Plan.

(195) SSC reserves the right to audit and perform spot checks at any time on the Contractor's operations and service management to ensure compliance to this Contract.

4.2 Service Continuity

(196) The Contractor must implement the Service Continuity Plan (all processes, procedures, roles, and responsibilities) within 60 FGWDs following completion, and service acceptance by SSC of the ORP, and provide the test results to SSC within 10 FGWDs of completion of the Service Continuity Plan testing.

(197) The Contractor must correct any problems identified during the testing of the Service Continuity Plan, which will be reviewed by the Technical Authority until all identified problems are agreed to be corrected.

(198) The Contractor must provide to SSC within 30 FGWDs of each anniversary date of the Contract any required updates to its Service Continuity Plan.

4.3 Contractor's IIS Service Desk

(199) The Contractor must provide a Service Desk for SSC to call for assistance 24 hours per day, 7 days per week, and 365 days per year.

(200) The Service Desk must accept emails from SSC' to a Contractor-provided mailbox with an auto reply to confirm receipt of the email.

(201) The Service Desk must acknowledge receipt of emails received from email addresses authorized by SSC within 15 minutes of receiving the email 24 hours per day, 7 days per week, and 365 days per year.

(202) The Contractor must provide the following telephone number(s) and associated Public Switched Telephone Network (PSTN) services for the Service Desk:

a) North American toll-free number(s);

b) TTY/ FAX/TDD (teletypewriter / telecommunications device for the deaf) access; and

c) Local number for the NCR if available.

(203) The Service Desk must answer calls (in person and pre-recorded messages) using the SSC's official language (French, English) requested by the caller in response to a message provided initially to the caller in both French and English that allows the caller to select their language of choice.

(204) The Contractor must monitor the service provided on a 24/7/365 basis and report immediately, any service affecting issues to SSC.

(205) The Contractor must provide support, on a 24/7/365 basis, to receive calls from SSC regarding service affecting issues.

(206) The Contractor must work cooperatively with the contact as specified in the work order or Service Order Request and SSC to resolve service affecting issues.

(207) The Contractor must notify SSC within 15 minutes of any service affecting issues detected or reported.

(208) The Contractor must track, monitor and report all service affecting issues.

(209) The Contractor must grant read access to authorized persons identified by SSC to the Contractor's trouble ticketing system, to facilitate the communication and update of information of service affecting issues.

(210) The Contractor must report by email or phone to SSC on the progress and status of the resolution of critical and service affecting issues every 30 minutes until the service is restored.

(211) The Contractor must attend meetings, to discuss and resolve issues regarding the performance of the services.

(212) When requested, Contractor's technical experts must attend the meeting.

(213) The Contractor must provide in advance, the name of the company and the individual who will be arriving on site.

4.4 Service Operation and Monitoring

(214) SSC reserves the right to audit and perform spot checks at any time on the Contractor's operations and service management to ensure compliance to this SOW.

(215) The Contractor must schedule new and additional installs, upgrades and service management activities including configuration changes (release or maintenance of the IIS) on Sundays between 12:00 AM and 6:00 AM local time. Exceptions are allowed on a case-by-case basis requiring approval from SSC.

(216) The Contractor must provide notification and work details, and must obtain approval from SSC 10 FGWDs in advance of the work to be done.

(217) The Contractor must coordinate new and additional installs, upgrades, and configuration and repairs of Services with SSC by:

(217.a) Calling before the actual start of work and identifying technician(s) performing the work;

(217.b) Calling to advise of delays in completion at the time at which the Contractor realizes that the work will extend past the predicted outage window;

(217.c) Calling to confirm completion of work and restoration of service; and,

(217.d) Submitting email notification of the description and completion status of the work to the Technical Authority.

(218) The Contractor must monitor and report all incidents on a 24/7/365 basis on the services provided to SSC.

(219) The Contractor must provide support on a 24/7/365 basis to receive calls from SSC regarding service issues.

(220) The Contractor must work cooperatively with SSC and other IIS Contractor, to resolve service incidents and problems.

(221) The Contractor must notify by email or phone to SSC within 15 minutes of any service problems detected or incidents reported.

(222) The Contractor must use a trouble ticketing system to track, monitor and report all service incidents and problems.

(223) The Contractor must grant read access to SSC to the Contractor's trouble ticketing system to facilitate the communication and update of information of service incidents and problems.

(224) The Contractor must report by email or phone to SSC on the progress and status of the resolution of service problems and Incidents especially those related to security, every 30 minutes until the service is restored and Incidents mitigated.

(225) The Contractor must attend meetings at locations determined by SSC, given 3 days advance notice, to discuss and resolve issues regarding the performance of the Services. When requested, Contractor's technical experts must attend the meeting.

(226) The Contractor must also provide SSC with Contractor's IIS router configuration (with passwords removed) in hardcopy and encrypted electronic format within 24 hours of a change being made to the router's configuration.

4.5 Security Assessment and Authorization

(227) The Contractor must apply throughout the System life Cycle of the IIS:

d) A mature operations and maintenance process that supports performance of security testing, vulnerability assessment, and risk assessment reports, change and configuration management to ensure that it maintains the security posture of the IIS; and

e) A mature disposal process to ensure the secure disposal of sensitive IT assets related to IIS.

(228) The Contractor agrees that Canada may audit the Contractor's compliance with the security requirements included in the Contract at any time. Canada will provide the Contractor with advance notification of any such audits.

(229) The Contractor shall provide Canada with full access to its premises, its network, and all databases or data related to the IIS Contract at all reasonable times, if requested by the Contracting Authority.

(230) The Contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this audit.

(231) If Canada identifies any security deficiencies during an audit, the Contractor shall correct the deficiencies at its own expense within an agreed timeframe with Canada.

(232) The Contractor throughout the System Life Cycle of the IIS shall:

a) Mitigate risks to an acceptable level as determined by Canada.

b) Establish and document risk acceptance levels based on risk criteria in accordance with resolution time frames as agreed by Canada.

c) Undergo security assessment and authorization as per provisions of the Contract.

d) Seek authorization for operations by Canada following all changes to the IIS infrastructure within the Contractor's control, to the extent required to carry out a program of inspection to safeguard against threats and hazards to the confidentiality, integrity, and availability of Canada data, the Contractor shall afford Canada access to the IIS Service Facility, installations, technical capabilities, operations, documentation, records, databases, logs, reports, and scan results within 72 hours of request by Canada. This includes processes related to both security assessment and authorization and continuous monitoring.

(233) The program of inspection shall include, but is not limited to:

a) Authenticated and unauthenticated operating system/network vulnerability scans;

b) Authenticated and unauthenticated web application vulnerability scans; and

c) Authenticated and unauthenticated database application vulnerability scans.

(234) The Contractor agrees that automated scans can be performed by Canada personnel, or agents acting on behalf of the Canada, using Canada operated equipment, and Canada specified tools.

5 MANAGEMENT SERVICES

(235) The Contractor must provide all components required to perform Management Services for the IIS, at no additional cost to SSC.

(236) The Contractor must provide Management Services for the IIS at no additional cost to SSC.

(237) The Contractor must use a secure (encrypted) and trusted connection, which includes strong authentication and auditing of user access along with, non-repudiation of changes and data integrity protection, for remote management and administration of IIS Managed Services, using a process approved by SSC. The Contractor shall make the associated audit logs available to SSC upon request.

(238) The Contractor must schedule service management activities including configuration changes (release or maintenance of Service) on Sundays between 12:00 AM and 6:00 AM local time. Exceptions are allowed on a case-by-case basis requiring approval from SSC.

(239) The Contractor must provide notification and obtain approval from SSC 10 FGWDs in advance of the work to be done.

(240) The Contractor must deliver the following Management Services for the IIS 24 hours per day, 7 days per week, 365 days per year:

a) Service Order Management

b) Change Management;

c) Configuration Management;

d) Incident Management;

e) Release Management;

f) Capacity Management; and

g) Availability Management.

5.1 Change Management

(241) A Change Request must be created by the Contractor and submitted to SSC for all changes to the hardware, software, applications and processes used by the Contractor to deliver the IIS.

(242) All Change Requests must be approved by SSC.

(243) Changes to the Contractor's network and support system infrastructure that are unrelated to IIS delivered to SSC do not have to be approved by SSC.

(244) The Contractor must create at least 1 Change Ticket for each Change Request submitted by SSC within 1 FGWD of receiving the Change Request.

(245) The Contractor must accept Change Requests from SSC 24 hours per day, 7 days per week, 365 days per year using email, to a Contractor-provided mailbox with an auto reply to confirm receipt of the email.

(246) The Contractor must implement Change Requests, excluding Emergency Changes, during maintenance windows as approved by SSC.

(247) The Contractor must escalate Change Requests as requested by SSC.

(248) The Change Tickets must include, but not be limited to, and the Contractor must update as necessary, the following dedicated information fields for all Change Requests:

a) Ticket number;

b) Change description;

c) Related Change Tickets;

d) Type;

e) Status (i.e., open, closed, in progress, approved, suspended, cancelled, unsuccessful, failed, etc.);

f) SSC's Change Ticket number;

g) Contractor's contact information (name, telephone number and email address);

h) Client Organization identifier;

i) SSC's contact information (name, telephone number and email address);

j) Activity log

k) Scheduled date and time of change;

l) Completion date and time of change;

m) Change approver's name; and

n) Back-out procedures.

(249) The Contractor must revise the contents of the Change Ticket information fields or change acceptance test plan as requested by SSC.

(250) The Contractor must update the status of a Change Ticket (failed, unsuccessful, successful) as specified by SSC based on acceptance testing for the change and back-out procedure results (if back-out implemented).

(251) The Contractor must provide Change Ticket information by email to a pre-defined distribution list specified by SSC for Change Requests specified by SSC until the

associated Change Tickets are closed or SSC cancels the automatic update reporting based on changes to the Change Tickets' status.

(252) The Contractor must back-out changes, when requested by SSC, using the back-out procedures specified in the Change Ticket that includes:

a) The tasks and activities to return the service (functionality and data) back to its pre-change state;

b) The expected operational results after the back-out has been executed;

c) The criteria to verify that the back-out was successful; and

d) Reporting the back-out results in the activity log of the Change Ticket.

(253) The Contractor must back-out changes, when the acceptance criteria specified for a Change Request are not met post implementation, using the back-out procedures specified in the Change Ticket.

(254) The Contractor must provide a Change Request Implementation Notice to SSC, no later than 48 hours in advance of the implementation of the Change Request, when the Contractor has assessed, approved and made all required preparations to implement the Change Request.

(255) The Contractor must provide a Change Request Cancellation Notice to SSC, within 24 hours of cancellation of the Change Request by the Contractor.

(256) The Contractor must perform acceptance testing of the change using the Acceptance Test Plan, specified in the Change Ticket, approved by SSC and report the acceptance testing results in the activity log for the Change Ticket.

(257) The Contractor must provide acceptance-testing results in the Change Ticket, within 2 FGWDs after the completion of a Change Request.

(258) The Contractor must successfully complete the Acceptance Test Plan in the Change Ticket before the Change Request is accepted by SSC.

(259) The Contractor must close the Change Tickets for a Change Request after the Change Request has been accepted by SSC.

(260) The Contractor must provide a Change Request Completion Notice to SSC within 2 FGWDs of the completion of any Change Request.

(261) The Contractor must allow SSC to access Change Tickets using a web browser that includes:

a) Viewing individual Change Tickets in a hierarchical fashion where information within a ticket can be viewed in a successive "drill-down" manner (i.e., related tickets); and

b) Viewing open or closed Change Ticket summary information, displayed in graphical and tabular format, by year, month, day and hour intervals over a time period selected by SSC for number of tickets by type, and status.

5.2 Configuration Management

(262) Configuration Management performed by the Contractor for the IIS must include:

a) The configuration and programming of all features and functions and modifications of hardware and software components to meet the on-going operational requirements of the IIS in accordance with SSC's requirements;

b) Implementing hardware and software fixes;

c) Maintaining configuration information and status on all hardware and software components;

d) Backing up configuration files, incremental changes on a daily basis, and maintaining the backup configuration files off-site;

e) Maintaining configuration log files that will include an entry for each configuration change where each entry in the configuration log file must include:

i) Date and time of configuration change; and

ii) Resource making the configuration change;

f) Providing the configuration information of hardware and software components when requested by SSC within 5 FGWDs of a request, in a file naming convention as specified by SSC and Commercial Off-the-Shelf (COTS) file format that is approved by SSC;

g) Maintaining the current and previous copies of configuration information; and

h) Tracking the status of a configuration item as it changes from one state to another (e.g. for instance 'under development', 'being tested', 'live', or 'withdrawn').

5.3 Incident Management

(263) The Contractor must work co-operatively with SSC and any other third parties as requested by SSC to resolve incidents, problems and issues quickly and effectively, by prompt response times and resolution.

(264) The Contractor must work with SSC to establish direct communication between specialists and technicians of SSC and the Contractor, to minimize resolution through troubleshooting and fault isolation to find root cause and acceptable workaround of a reported incident.

(265) The Contractor must escalate incidents, if an incident has remained open, based on clear and well-established escalation levels, procedures and processes.

(266) The Contractor must provide SSC with an Operational and Management Escalation Matrix, within 5 FGWDs of a request by SSC, that defines the personnel, with alternates (of equal authority) for a minimum of 5 Escalation Levels (Escalation Level 1 to Escalation Level 5, where Escalation Level 5 is the most senior personnel), and contains clear contact instructions.

(267) The Contractor must provide SSC with notification of incidents according to the operational and management escalation matrices.

(268) The Contractor must change the Escalation Level for incidents within 15 minutes of a request by SSC.

(269) The Contractor must create an incident ticket for each incident.

(270) The Contractor must log all privacy or security violations and other security related events as incidents.

(271) The Contractor must automatically provide Incident Ticket information by email to a pre-defined distribution list specified by SSC for incidents selected by SSC until the incident is closed or SSC cancels the automatic update reporting based on changes to ticket status.

(272) The Incident Tickets must include, but not be limited to, and the Contractor must maintain, the following dedicated information fields for all incidents:

a) Ticket number;

b) Incident description;

c) Incident originator (Contractor, SSC);

d) Related incident tickets;

e) Related Change Tickets;

f) Date and time stamp when incident initiated;

g) Date and time stamp when incident closed;

h) Incident type (production, functional testing, performance testing, security, etc.) as specified by SSC;

i) Incident severity;

j) Incident status (i.e., open, closed, in progress, suspended, cancelled, etc.);

k) SSC's ticket number;

l) Service function impacted;

m) Service Desk contact to initiate ticket (name, telephone number and email address);

n) Contractor's contact information (name, telephone number and email address);

o) Client Organization/User identifier (as specified by SSC);

p) Client Organization/User type (as specified by SSC);

q) Client Organization/User language; and

r) Department's contact information (name, telephone number and email address).

(273) The Contractor must open an incident ticket within 5 minutes for both Contractor-determined and SSC-reported incidents.

(274) The Contractor must update the incident ticket information log following a change in status.

(275) The Contractor must document all management and technical escalations for incidents in the incident ticket information log.

(276) The Contractor must, within 15 minutes of detection (24 hours, 7 days, 365 days), notify SSC via phone and email of any suspected or actual security incidents, including unauthorized intrusions, denial of service attacks, fraud detection, and all other security breaches.

(277) The Contractor must track and report the outage time of each incident in the associated Incident Tickets.

(278) The outage time for an incident must start at the time that the incident is detected by the Contractor or reported to the Contractor by SSC.

(279) The outage time for an incident must stop at the time that the IIS is fully restored for that incident and SSC has approved the closure of the associated incident tickets.

(280) The Contractor must suspend an incident (Incident Ticket resolution outage timer placed on hold) at SSC's request.

(281) An incident suspended by SSC must remain suspended until released by SSC or for a fixed time period specified by SSC.

(282) The Contractor must not suspend an incident without approval from SSC except when the Contractor requests information from SSC necessary to resolving an incident and SSC is unable to provide the information.

(283) The Contractor must release (Incident Ticket resolution outage timer is started from the time it was suspended) an incident suspended by the Contractor where the requested information is communicated by SSC to the Contractor.

(284) The Contractor must suspend outage time for an incident at SSC's request or where the Contractor has requested closure of an incident Ticket pending SSC's approval and SSC is not available to consider the request.

(285) The Contractor must restart the outage time for an incident where the outage time has been suspended when requested by SSC or when SSC is available to review the request to close an incident and has determined that the Incident must remain open.

(286) The Contractor must obtain SSC's approval before closing an incident.

(287) The Contractor must close the Incident Tickets after SSC has approved closing the Incident.

(288) The Contractor must notify SSC of the resolution of an incident according to severity as specified by SSC.

(289) If an incident is closed and a subsequent Incident occurs within 24 hours for the same problem, the Contractor must re-open the original Incident or open a new Incident with a cross reference to the previous Incident and report the start time against the original Incident.

(290) The Contractor must identify and document the causal factors (root causes) of all Incidents.

(291) The Contractor must develop workarounds to address all identified root causes.

(292) The Contractor must designate 3 or more Incidents with the same root cause within a rolling 90-day window as a Chronic Problem.

(293) The Contractor must assign the next highest severity for Incidents designated as chronic problems.

(294) The Contractor must link Incidents to existing or new Chronic Problems as requested by SSC.

(295) The Contractor must allow SSC to access Incident Tickets using a web browser that includes:

a) Searching and sorting for open and closed Incident Tickets based on any Incident Ticket field over a reporting period (start/end date) and time interval (year, month, week, day, hour) selected by SSC;

b) Downloading Incident Ticket search results in a file naming convention specified by SSC and COTS file format that is approved by SSC;

c) Viewing individual Incident Tickets in a hierarchical fashion where information within a ticket can be viewed in a successive "drill-down" manner (i.e., related tickets); and

d) Viewing open or closed Incident Ticket summary information, displayed in graphical and tabular format, by year, month, day and hour intervals over a time period selected by SSC for number of tickets by type, severity, and status.

5.4 Release Management

(296) Release Management must include:

a) Integration with the change, incident and configuration management processes;

b) Planning, testing, and implementing the rollout of new and changed software and hardware.

(297) The Contractor must provide release notes for any IIS release within 40 FGWDs prior to the implementation of the release.

(298) The Contractor must not implement any releases for the IIS without prior approval from SSC.

(299) The Contractor must participate in release management review meetings conducted by SSC to discuss upcoming IIS releases as requested by SSC.

5.5 Capacity Management

(300) Capacity Management for IIS must include:

a) Reviewing and analyzing service performance statistics and service levels to identify capacity shortfalls or issues;

b) Adapting, tuning, and improving services to ensure optimal use and performance;

c) Assessing IIS's capacity requirements and providing recommendations for capacity changes to services.

5.6 Availability Management

(301) The Contractor IIS must respond to any failure situation to ensure Internet access availability.

(302) Availability Management must include:

a) Reviewing availability requirements and ensuring contingency plans are put in place and tested on a regular basis to ensure service delivery requirements are met;

b) Proactively identifying availability issues so they can be resolved before they impact the IIS;

c) Analysis of availability data to identify availability issues; and

d) Configuring services to ensure contracted availability.

(303) The Contractor must report to SSC as part of weekly operational review meetings issues that could affect availability or lead to capacity shortfalls including proposed solutions to ensure contracted availability.

(304) The Contractor must notify SSC of scheduled outages of the IIS at least 20 FGWDs in advance of a scheduled outage.

(305) The Contractor must obtain SSC's approval for any scheduled outages of the IIS.

6 MEETINGS

(306) Meetings must be conducted during business hours (08:00 to 17:00 ET) of FGWDs in Ottawa, Ontario, SSC in person unless otherwise indicated by SSC.

(307) SSC may organize and conduct a contract review and planning meeting on a quarterly basis. The Contractor must attend this meeting at SSC's request.

(308) The contract review and planning meetings may include a review of the following elements in relation to the Work:

a) Service management performance for the preceding quarter;

b) Major service delivery and service support issues in the preceding quarter;

c) Major planned improvements to service delivery and service support in the upcoming quarter; and

d) Risks, opportunities, and goals in the upcoming quarter.

(309) The Contractor must organize and participate (using teleconference or other means as specified by SSC) in operational review meetings. The frequency of these meetings will be agreed upon between SSC and the Contractor after Contract Award. These meetings will occur monthly as a minimum or more frequently, depending on the volume and severity of operational matters to be dealt with. These meetings will be to review service affecting issues and the outcome of changes applied since the previous operational review meeting, to review any issues that have occurred since the last operational review meeting, the progress of issue responses that are currently under way, and the approval and planning of corrective action recommended in Root Cause Analysis (RCA) reports.

(310) The Contractor must organize and participate (using teleconference or other means as specified by SSC) in Change Management Meetings, as requested by SSC, to review the outcome of Change Requests applied during the previous week, Change Requests scheduled for the next week, and Change Requests submitted by the Contractor for SSC's approval.

(311) The Contractor must organize and participate (using teleconference or other means as specified by SSC) in a Service Level Management Review meeting every 3 months, during which Service Level attainment for the previous 3 months is reviewed. For this meeting, the Contractor must be prepared to discuss any Service Level failures, describe steps taken to forestall repetition of service affecting conditions, and discuss service evolution plans for the next 3 months.

(312) The Contractor must organize and participate in weekly meetings to review new and outstanding SORs.

(313) The Contractor must make available all relevant resources to be present at meetings or be able to communicate with them through teleconferencing or other means, during these meetings.

7 REPORTS AND DOCUMENTATION

(314) The Contractor must provide all required documents and reports identified in this SOW, including the documents listed and described in this Section.

(315) The Contractor must provide all IIS documentation and reports in English and COTS file format approved by SSC.

(316) The Contractor must post reports electronically in the respective EIET for access and download by authorized persons as specified by SSC

(317) The Contractor must track versions and change history for changes to IIS reports and documentation.

(318) The Contractor must archive data for all IIS reports for the period of the Contract, and at SSC's written request, provide to SSC within 20 FGWDs the requested data in a file format and file naming convention specified by SSC.

(319) The Contractor must not require the use of ActiveX components for access to IIS reports and documentation.

(320) Unless otherwise indicated for a specific report in the SOW, the Contractor must provide monthly reports 5 FGWDs following the previous reporting month.

(321) The Contractor is responsible for maintaining the information accuracy and delivering updated documentation within 5 FGWDs of any changes or updates to SSC.

(322) The Contractor must update IIS documents and diagrams following a change that:

a) Affects the information described in the IIS document and diagram; or

b) Is required by SSC to accept the IIS document and diagram.

(323) The Contractor must provide Post Mortem Reports that includes Lessons Learned regarding problems encountered. These reports must be posted on the EIET and remain available and accessible through archives, for the duration of the Contract Period.

(324) The Contractor must provide inventory reports by service type and location, accessible by the Technical Authority from the EIET, as described under Section 7.3 Configuration Document.

7.1 Monthly Reports

(325) The Contractor must provide a monthly report to SSC on the status of the Contract that includes:

a) Service Level issues requiring resolution;

b) Risks including probability and mitigating actions;

c) Billing disputes requiring resolution.

(326) The Contractor must provide a monthly report to SSC in tabular and graphical format that includes for each instance where a Service Level was not met:

a) Calculated Service Level;

b) Contracted Service Level;

c) A description of failure to meet the Service Level; and

d) Applicable Service Credits.

(327) The Contractor must provide a monthly Financial Expenditure report to SSC.

7.2 Reports by Special Request

(328) The Contractor may be requested to provide a special report to SSC, for a reporting period specified by SSC, on security breaches that includes:

a) Number of security Incidents and actions taken;;

b) Number of security investigations completed;

c) Average/highest response time to security Incidents; and

d) Average/highest security investigation completion time.

(329) The Contractor may be required to provide special reports for all high severity Incidents that includes tracking and follow-up of outstanding items for the Incidents.

(330) The Contractor may be required upon special request to provide to SSC a special inventory report on equipment implemented at SSC's sites for the IIS, within 10 FGWDs of a change to the information from the previous report, that includes:

a) Equipment owned by the Contractor;

b) The manufacturer of the equipment and country of origin;

c) The model and serial number of the equipment;

d) The date that the equipment was installed; and

e) The date on which the Firmware was last updated.

(331) The Contractor may be required to provide management reports to SSC on operations status that include:

a) Executive overview and summary on the overall service;

b) 13 month graphical and tabular report view of:

i) Target value, actual value, and number of exceptions for each Service Level;

ii) Number of Change Requests submitted, failed, and completed;

iii) Minimum, maximum, and average time between the scheduled and actual implementation times to complete Change Requests;

iv) Number of Incidents; and

v) Minimum, maximum, and average time to open and close Incident by severity and type;

c) Summary of emergency Change Requests;

d) Details of Incidents and Change Requests where the escalation process failed or was not followed;

e) Description of the corrective actions and timeframes to implement any required changes to prevent future Service Level failures; and

(332) The Contractor may be required to provide reports to SSC for chronic problems that:

a) Describe the chronic problems;

b) Steps taken to resolve the chronic problems; and

c) Recommendations as to how similar chronic problems may be avoided in the future.

(333) The Contractor may be required to provide reports to SSC for each Service Level that include:

a) Daily aggregated Service Level data for the past 60 days,

b) Daily aggregated Service Level data for the past 13 months; and

c) Monthly aggregated Service Level data since Contract award,

7.3 Configuration Document

(334) The Contractor must provide an IIS Configuration Document that describes the design and configuration of the equipment and facilities deployed by the Contractor to provide the IIS.

(335) The document must contain a graphical physical overview of the portion of the Contractor's network used to supply the service to the SSC Intranets, identifying each of the routers and nodes, interfaces to external networks.

(336) The Contractor must maintain and update their respective IIS Configuration Document for the Contract period. Any revisions to the document are subject to approval by SSC.

(337) The IIS Configuration Document must, at a minimum, contain the following information:

(337.a) A graphical physical overview of the portion of the Contractor's network used to supply the IIS to the GC.Net, identifying each of the routers and nodes, interfaces to external networks, as well as telecommunications facilities used to interconnect them;

(337.b) Telecommunications facility capacity along with the performance thresholds for high availability and diversity requirements;

(337.c) The configuration of the interface of the Contractor's IIS Router, with passwords being deleted;

(337.d) Description of the Internet Interconnection at Network Access Points, Metropolitan Area Exchanges and network peering (IPv4 and IPv6) arrangements with the Contractor interface addresses;

(337.e) A block diagram showing the connectivity between the Contractor's network and other directly connected AS including any inter-AS connections not implemented using BGP 4;

(337.f) A description of any Contractor-specific special meanings or functionality pertaining to BGP attributes (e.g. special values or meanings for the "community" attribute);

(337.g) A description of how the Contractor reduces or eliminates the flow of routing information to the GC.Net by selective announcement of route information (i.e. route or path filtering or similar mechanisms); and,

(337.h) A description of how the Contractor implements transit facilities for GC.Net network numbers including where and how the Contractor maintains the routing register, how the Contractor enables transit IP traffic for the GC.Net network, any filtering (other than route or path filters) and any Contractor-specific features (e.g. the "advisory" RIPE attribute) that may have an effect on routing behaviour, and a description of the administrative procedures used to inform the upstream service provider of desired changes.

(338) The Contractor must maintain information accuracy and update their respective IIS Configuration Document for the life of the Contract.

(339) The Contractor must deliver the updated documentation within 5 FGWDs of any changes or updates.

(340) Any revision of the IIS Configuration Document is subject to approval by SSC.

8 MANAGEMENT REPORTING

8.1 Electronics Information Exchange Tool (EIET)

(341) The Contractor must provide SSC with a secure and reliable Electronics Information Exchange Tool (EIET) or equivalent, approved by SSC immediately after the contract award.

(342) The Contractor must make the EIET available for use within 60 FGWD days of Contract award.

(343) The Contractor's EIET must host or provide access to information such as Service Level Reports, technical and operational documentation, testing results, and electronic service invoices.

(344) The Contractor must protect the confidentiality of hosted information by restricting access to only authorized persons approved by SSC.

(345) If the Contractor's approved EIET is a Web Portal or other equivalent application:

(345.a) The Contractor must create and manage user accounts for individuals authorized by SSC when requested.

(345.b) The EIET must log all access automatically and the Contractor must provide the access logs to SSC when requested.

(345.c) The Contractor's EIET must enforce the following password requirements for user log in:

(345.c.1) Contain at least 6 characters;

(345.c.2) Change required every 60 days; and

(345.c.3) Contain upper and lower characters with at least 1 numerical symbol.

(345.d) The Contractor must lock down access to the EIET by IP addresses and application port numbers.

(345.e) The Contractor must implement Transport Layer Security (TLS) on the EIET and encrypt the web session using 3 Key Triple Data Encryption Algorithm (3DES) or Advanced Encryption Standard (AES).

(346) The Contractor must protect the EIET and its information according to industry standards and best practice such as using intrusion detection systems, antivirus software, firewalls and IP filtering routers.

(347) The Contractor may request deviations from this design or propose an alternate security perimeter design but are subject to approval by SSC.

(348) The Contractor must provide an EIET that will allow SSC to execute, view and download reports.

(349) The Contractor must provide reports available in HTML, CSV and XML formats or other formats approved by SSC.

(350) The Contractor must provide SSC with the ability to configure and define reports, based on the information system provided.

(351) The Contractor must allow SSC the option to enable mitigation or disable mitigation against a Denial of Service (DOS) event on the EIET.

(352) The Contractor must post on their EIET within 5 FGWD, the new updates related to a proposed change that has been approved under the Change Management process, described in Section 5.2.

8.2 IP Traffic Data

(353) The Contractor must provide real-time reporting of IP traffic data on the EIET.

(354) The Contractor must store 5-minute aggregate IP and separate IPv4 and IPv6 traffic data for the last 14 days and this data must be available for query on the EIET.

(355) The Contractor must store 30-minute aggregate IP and separate IPv4 and IPv6 traffic data for the last 8 weeks and this data must be available for query on the EIET.

(356) The Contractor must store 2-hour aggregate IP and separate IPv4 and IPv6 traffic data for the last 6 months and this data must be available for query on the EIET.

(357) The Contractor must monitor and record both inbound and outbound IP traffic usage at their respective SIP from the GC.Net every 5 minutes, 24 hours/day, 7 days/week and 365 days/year (24/7/365)

8.3 Anti-Denial of Service Reports

(358) The Contractor must provide reports on the Anti-Distributed Denial of Service that will:

(358.a) Be available in HTML, XML, CSV and XML formats or other formats approved by SSC.

(358.b) Be automatically sent on a periodic basis to specific email addresses provided by SSC.

(358.c) Show application IP traffic in and out of the network for the top 100 applications broken down by application port for TCP and UDP Protocol (e.g. http, https, smtp) summary IP traffic broken down by IP protocol.

(358.d) Showing the top 100 addresses consuming the most bandwidth as a Top Talker Summary Report.

(358.e) Show information about the worms and infected hosts in the network as a Worm Activity Report.

(358.f) Show information on the scrubbing of IP traffic as a Threat Mitigation Report.

(358.g) Provide information on the amount of IP traffic flowing in, amount of IP traffic dropped and the amount of IP traffic passed through.

8.4 Operations Management Procedures

(359) The communications between the Contractor and SSC must be coordinated and flow through Canada.

(360) The Contractor must communicate routine day-to-day operational and service management information with the NOC and SSC Service Desk as well as coordinate related activities through designated and authorized contacts, once formalized through SSC.

(361) The Contractor's Operations Management Procedures must describe in detail the respective Contractor's processes and procedures regarding service operations and delivery to SSC.

(362) The Contractor must provide SSC with Operations Management Procedures as outlined by the headings in each of the following sub-sections:

8.4.1 Incident and Problem Management

(362.a.1) Trouble ticketing system and processes,

(362.a.2) Incident handling flowchart,

(362.a.3) Incident Reporting and Notification Escalation Procedures,

(362.a.4) Resolution times, and

(362.a.5) Root Cause Analysis.

8.4.2 Contractor's Helpdesk and Support Organization

(362.a.6) 24 /7/365 access and support, and

(362.a.7) Helpdesk telephone and e-mail contact information

8.4.3 Change Management Procedures and System

(362.a.8) Handling of Types of Changes (Emergency, Maintenance, Release),

(362.a.9) Flowchart of ordering and provisioning process, and

(362.a.10) Turnaround timeframes.

8.4.4 Security Management Procedures

(362.a.11) Contractor's Corporate Security Policy,

(362.a.12) Security Control Systems, and

(362.a.13) Personnel Security Clearances, whereby the Contractor must obtain personnel security (SECRET) clearances and Canadian Citizenship for their employees, individuals and any subContractor personnel, involved in providing the service to GC, including conducting the management, administration and support of those components.

8.5 Service Management Procedures

The Contractor must provide to SSC with the respective Contractor's Service Management Procedures that describes in detail the Contractor's service management processes. The Service Management Procedures must include:

(362.b) A list of the service measurements reported for each service;

(362.c) The method and frequency used for service measurements;

(362.d) Calculations used to derive reported Service Level values;

(362.e) A summary of Service Level Report formats used; and

(362.f) Service Level Objectives and Guarantees (if applicable) for each service.

8.6 Service Level Reports

(363) The Contractor must deliver the required monthly Service Level Reports to SSC by the tenth day of the following month for review and approval. The Service Level Reports document the service performance through monitoring and measurements.

(364) The Contractor must post the Service Level Reports in electronic format on their EIET. The reports must include:

(364.a) The Contractor's service performance values;

(364.b) Trouble ticket report of service incidents and problems, describing the incident, issues, diagnosis, corrective actions and resolution time; and,

(364.c) Order provisioning report that provides the description, date started, and date completed of the orders in progress and completed.

(365) When requested by SSC, the Contractor must provide within 5 FGWDs a written root cause analysis and report on the failed service delivery describing the incident, diagnosis, problem, corrective action and mitigation strategy to prevent a similar incident from occurring.

8.7 Service Order Requests

(366) The Contractor must provide the capability to process and track Service Order Requests through the EIET.

8.8 Interface Control Document (ICD)

(367) The Contractor must provide ICD documents that contain the service information of the technical interface between the Contractor IIS and SSC Intranets.

(368) SSC will provide a blank ICD template to the Contractor after the Contract Award. When completed, the document will include all the information required by the Contractor and the SSC Intranet to implement and support the interface.

(369) The Contractor must provide the following information in their ICD:

(369.a) Contractor's contact information;

(369.b) A description of the physical layer of the IIS;

(369.c) A description of the data link layer of the IIS including data link encapsulation protocols and settings;

(370) The Contractor must ensure that its input into the ICD is accurate and current;

(371) The Contractor must provide changes or updates to the ICD within 3 FGWDs; and

(372) The revised ICD will be re-issued by the Contractor and provided to SSC for review by the Contractor.

8.9 Security

(373) The Contractor must provide online audit records for the IIS at sites specified by SSC, to SSC within 1 FGWD of a request by SSC, in a COTS file format specified by SSC.

(374) The Contractor must provide archived audit records for the IIS at sites specified by SSC, to SSC within 5 FGWDs of a request by SSC, in a COTS file format specified by SSC.

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

(376) The Contractor must allow SSC, at no cost to SSC, within 10 FGWDs of a request by SSC, to enter the Contractor's premises to inspect and audit the Contractor's compliance with the privacy, security and information management requirements under the Contract and to have full access to all Personal Information and Records during FGWDs from 08:00 to 17:00 ET.

(377) In the event of a security incident, or as otherwise requested by SSC, the Contractor must co-operate with any security audits or inspections requested by SSC by providing the requested information within 10 FGWDs of the request:

(378) The Contractor must provide access to the Contractor's facilities and systems and provide sufficient evidence and documentation in a timely manner when requested by SSC.

(379) The Contractor must address, within the timeframe specified by SSC, any risks identified in SSC's security and privacy compliance processes that demonstrate that the security and privacy of SSC, has been compromised or has the potential to be compromised.

8.10 Conformance Review

(380) SSC may, on an annual basis, conduct a conformance review that includes, but is not limited to:

a) Ensuring the IIS conforms to the IIS Security Requirements;

b) Ensuring that all IIS software has current and up-to-date security updates and patches for all known vulnerabilities;

c) Ensuring that the Contractor is proactively monitoring for software vulnerabilities in IIS and implementing any required security patches and/or software releases to remedy such vulnerabilities; and

d) Ensuring that the Contractor is reviewing security audit log records on a daily basis.

(381) The Contractor must provide supporting evidence within 10 FGWDs of a request by SSC for any supporting evidence required for the conformance review.

(382) If SSC deems that the supporting evidence does not support the conformity to the Contract, SSC will request a plan from the Contractor to address the discrepancies identified by SSC with conformity to the terms and conditions of the Contract.

9 SERVICE QUALITY MANAGEMENT

(383) The Contractor must have a Service Quality Management framework for management of their service performance in terms of service levels, Service Level Management Plans and Service Level Reporting as well as service orders, operation, monitoring, reporting, documentation and billing.

(384) The Contractor must take the necessary measures on its interfacing equipment or infrastructure to maintain service levels.

(385) The Contractor must provide an Internet Interconnection Service in accordance with the service levels defined as a set of service performance requirements, detailed in Table 7, of Service Level Management section.

(386) The Contractor must monitor and measure service levels 24 hours per day, 7 days per week, and 365 days per year.

(387) The Contractor must provide any hardware and/or software that are necessary to monitor and measure service levels.

(388) The Contractor must calculate and report service levels to two decimal points, unless otherwise indicated for a service level.

(389) The Contractor must provide SSC with access to the information from its service management information and reporting tool(s) for monitoring service level parameters that are critical for the service quality and delivery.

(390) The Contractor must provide the IIS and the Anti-DDOS service at availability levels of 99.5% measured over a calendar month, on a 24/7/365 basis.

(391) The "availability" is a percentage function based on the cumulative outage periods and the total time the IIS is available as follows:

(Expected Service Availability for the Month – Cumulative Outage for the Month) X 100% / Expected Service Availability for month

(392) The Contractor must provide written justification or proof upon failure to meet any service levels. SSC is preauthorized to accept written justification for outages due to any of the following:

a) The failure of telecommunication links or equipment, not provided by the Contractor;

b) Scheduled maintenance interruptions approved by SSC;

c) Action by a person or persons outside the control of the Contractor; or Contractor is delayed access or denied access to GC premises should physical access be required to repair or restore the service.

10 SERVICE LEVEL MANAGEMENT

10.1 Service Level-Internet Availability (SL-IAV)

(393) The SL-IAV for the IIS is the Service Level for the Internet Interconnection and the Anti-DDoS Availability whereby the Contractor is expected to ensure the service is available minimizing outages as defined in Table 7 – IIS Service Levels.

10.1.1 Service Level-Maximum Service Outage Time (SL-MSOT)

(394) The SL-MSOT for the IIS and for the Anti-DDoS must be less than or equal to 216 minutes (60min.*24Hours*30Days*0.005) or approximately equivalent to 99.5% availability of accumulated outage time 24 hours per day for all days in any 1 (30 day) calendar month.

(395) The Contractor must calculate SL-MSOT for the IIS and the Anti-DDoS by summing the outage time for all incidents for that calendar month:

(396) The outage time will be excluded in the calculation of the SL-MSOT for the IIS for an incident involving configuration problems with work authorized by SSC.

10.1.2 Service Level-Maximum Time to Restore Service (SL-MTRS)

(397) The SL-MTRS for the IIS the Anti-DDoS is within 4 hours.

(398) The calculation of SL-MTRS begins from the time at which an incident of SL-MSOT is identified by SSC or the Contractor for the IIS and the Anti-DDoS, until the time that the Incident is closed.

(399) The calculation of SL-MTRS continues for each incident where the outage time occurs independently, whether or not the SL-MSOT has been exceeded in any calendar month.

10.2 Service Level-Service Order Response (SL-SOR)

(400) The SL-SOR for the IIS and the Anti-DDoS is the Service Level for Service Order Response whereby the Contractor is expected to fill orders within a specific period of time as specified in Service Order section of the contract. If the Contractor fails to deliver or misses on deliveries of Service Order Requests (SOR) in a monthly review

period, the Contractor must provide a credit on related charges for missed SORs in the following month.

10.3 Service Levels-Packet Data Throughput, Packet Transit Delay and Packet Loss

The parameters for data throughput, transit delay (SL-PTD) and packet loss (SL-DPL) are defined in Table 7 – IIS Service Levels.

10.4 IIS Service Level Table

Service Level Parameter	Descriptions	Service Level Requirement
Packet Data Throughput	▪ The contractor must measure the data throughput at the SIP at a minimum interval of every 5 minutes, 24/7/365 and report the measurement results on their web portal accessible by the TA.	In the event of a failure of one ISP, all traffic flowing to and from the Internet is rerouted automatically to and transmitted by the other ISP. As the Contractor will not be notified in advance of such failure, the contractor's IIS must respond to the situation automatically and smoothly to ensure the Internet availability. The contractor must always support additional IP traffic within the committed throughput.
Packet Transit Delay (SL-PTD)	▪ IIS-NAP transit delay (see Figure 2) – the contractor must measure the one-way transit delay using packet sizes of up to 576 bytes from their respective IIS interface to each NAP interface where the Contractor has peering arrangements with other ISPs. ▪ IIS-SIP transit delay – the contractor must measure the one-way transit delay using packet sizes of up to 576 bytes from the Contractor's IIS interface to the SIP. ▪ Round-trip transit delay tests are acceptable where each test result is divided in half in order to obtain the one-way transit delay. ▪ The Contractor record the packet transit delay for both traffic directions with a minimum sampling period of every 5 minutes, 24/7/365, and report the measurement results on their web portal accessible by the TA.	IIS-NAP transit delay – The contractor must provide the IIS with the one-way packet transit delay between the IIS interface and each NAP interface (within a 3000 km radius of the IIS interface within Canada and continental United States) is no more than 35 milliseconds for at least 95% of the packets within any single hour, including the busiest hour. IIS-SIP transit delay – The contractor must provide a guarantee that the IIS-SIP one-way transit delay is no more than 10 milliseconds for at least 95% of the packets within any single hour, including the busiest hour.

Table 7 – IIS Service Levels

Service Level Parameter	Descriptions	Service Level Requirement
Data Packet Loss (SL-DPL)	▪ The contractor must measure and record the Packet Loss from their respective IIS interface to each NAP interface for both traffic directions with a minimum sampling period of every 5 minutes, 24/7/365, and report the measurement results on their web portal accessible by the TA.	The contractor must provide the IIS service with the Packet Loss no more than 1% between the IIS interface and each NAP interface within any single hour.
Availability (SL-IAV)	▪ An outage is whenever GC.Net cannot communicate with the Internet due to failure from the respective Contractor's IIS or within the respective Contractor's infrastructure. ▪ The Contractor's measurements for packet transit delay will also be used to measure and monitor the respective Contractor's IIS availability. Should 2 consecutive transit delay test attempts fail to obtain a reply from a NAP interface, the Contractor must record this as the outage start time of the service on the trouble ticket. The IIS unavailable duration is accumulated from the outage start time until when the corresponding NAP interface replies to the transit delay test packet. Each outage period in each month is added together to obtain the total outage time of the IIS for the month.	▪ **SL-MTRS:** In the event of an outage, the Contractor must restore the IIS and the Anti-DDoS within 4 hours beginning at the recorded outage start time in the trouble ticket. ▪ **SL-MSOT:** The Contractor's IIS and the Anti-DDoS must be available at all times, with the exception of a maximum of 40 cumulative minutes of outages in any calendar month.

Table 7 – IIS Service Levels (Cont'd)

Internet Interconnection Service (IIS)

For

Shared Services Canada

Annex A - Appendix A: Definitions and Acronyms

Date: April 5, 2013 Version: D4

1 DEFINITIONS

Term	Definition
Address	Civic address where a Service Delivery Point (SDP) is located.
Denial-of-Service (DoS) attack	An attempt to make a computer or network resource unavailable to its intended users.
Authentication	A process that establishes that User has retained ownership or exerts control over the Credential that has been issued to them.
Availability Management	Process responsible for defining, analysing, planning, measuring and improving the availability of a service.
Canada NCA	A site within a radius of 100km from the Parliament of Canada where the service is implemented.
Canada North	A site on the 54th parallel and above where the service is implemented.
Canada South	A site below the 54th parallel, excluding Canada NCA, where the service is implemented.
Certificate	An electronic file in a format which is in accordance with ITU-T recommendation X.509 V3, such as EPF or Entrust supported crypto-token, and which contains a public key of a subscriber, which can be an individual or a device, together with related information that is digitally signed with the private key of the Certification Authority that issued the Certificate.
Certificate Revocation List	A list issued and maintained by the Certification Authority of the Certificates that are revoked before their pre-set expiry time
Certification	Evaluation of the security features of an IT system and other related safeguards to establish the extent to which a particular design and implementation meets a specific set of security requirements, made in support of the accreditation process.
Certification Authority	An entity trusted by one or more entities to issue and manage X.509 public key certificates and CRLs. Each CA within the GC PKI may issue certificates under a choice of policies based on the level of assurance to which the CA has been accredited.
Change Management	Standardized methods and procedures that are used for handling of all changes to an IT infrastructure/service to minimize the number and impact of any related incidents upon service.
Change Request	Request to make a change to the hardware, software, applications and processes used by the Contractor to deliver the service.
Change Ticket	Means to record a Change Request.
Computer Based Training	Means the computer based training (CBT) services provided by the Contractor including the provision of documentation.

Term	Definition
Configuration Item	A configuration item (CI) is any component of an information technology infrastructure that is under the control of configuration management. Configuration items (CIs) can be individually managed and versioned, and they are usually treated as self-contained units for the purposes of identification and change control.
Configuration Management	Standardized methods and procedures to control changes made to hardware and software components of a system throughout its lifecycle.
Credential	Unique physical or electronic identifier that is associated with an individual.
Emergency Change	A Change Request to operationally restore a service where the failure or degradation of the service severely impacts service delivery or to correct a security Incident.
FIPS Mode	A mode of the Cryptographic Module that employs only approved security functions (not to be confused with a specific mode of an approved security function, e.g., Data Encryption Standard Cipher-Block Chaining (DES CBC) mode). This means that when a module is in the "FIPS mode", a non-FIPS approved method shall not be used in lieu of a FIPS-approved method. The FIPS 140-2 validation certificate will identify the cryptographic module's "FIPS mode" of operation (source: FIPS 140-2).
Firewall	Technology barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.
Host	Means any IP addressable entity connected to an IP-based network.
Incident	An event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Incident Management	Standardized methods and procedures to restore a service to normal operation as quickly as possible and to minimize the impact on business operations.
Latency	Delays in packet transmission over a network between the point of ingress and the point of egress. The unit of latency is time, measured in milliseconds (ms).
Managed Service	Provision of a service to a Client where the supplier of the service has responsibility for delivery of the service and where the service must meet the Client's pre-defined service levels.
Management Services	Means services provided by the Contractor that includes: Change Management, Configuration Management, Incident Management, Release Management, Capacity Management and Availability Management.

Term	Definition
Maximum Service Outage Time	Maximum accumulated outage time attributable to 1 or more Incidents in a calendar month.
Maximum Time to Restore Service	Maximum time to restore the service following an Incident resulting in an outage.
Network Address Translation	The process of modifying IP address information in IP packet headers while in transit across a traffic routing device.
Personal Information	As defined in section 3 of the Privacy Act.
Privacy Impact Assessment (PIA)	An assessment that describes the personal information flows in a project, and analyzes the possible privacy impacts that those flows might have.
Release Management	Standardized methods and procedures for the integration and flow of development, testing, deployment, and support of the services being provided.
Security Breach	Unauthorized logical or physical access to an information system that has compromised the IT system's confidentiality, integrity or availability.
Security Requirements Traceability Matrix (SRTM)	A document used to ensure that all security requirements are included in the IT system and can be traced through the design, implementation and testing phases of the system development.
Security Testing	The processes to confirm that the technical security safeguards are functioning correctly
Security Validation	The process of establishing a correspondence, or mapping, between security requirements and the design elements or procedures that implement or address those security requirements.
Security Verification	The processes to confirm that proposed security safeguards and assurance requirements have been implemented correctly
Service Delivery Point	A location (i.e. civic address) where an instance of the service is implemented.
Service Design	Means the service design prepared by the Contractor for each Service Project.
Service Desk Response	Time required for the Contractor's Service Desk agent to answer a call.
Service Level	Value that is used to assess the performance, availability or quality of service, product or system.
Service Level Change Request Response	Means the service level for the response time to a change request.
Service Level Maximum Service Outage Time	Means the service level for the maximum time of a service outage.

Term	Definition
Service Level Maximum Service Outage Time (SL-MSOT)	Means the service level for the maximum outage time for the service being provided.
Service Level Maximum Time On-Site	Means the service level for the maximum time elapsed for a technician to arrive on-site once a problem has been reported.
Service Level Maximum Time to Restore Service (SL-MTRS)	Means the service level for the maximum elapsed time to restore the service, once a problem has been reported.
Service Level Operations Centre Availability	Means the service level for the availability of the Operations Centre.
Service Level Performance	Means the service level for Data Throughput, Packet Transit Delay and Packet Loss.
Service Level Service Order Response	Means the Service Level for the response time to a Service Order Request.
Service Level Service Portal Availability	Means the service level for the availability of the service portal.
Service Management Plan	Plan that specifies the management services to be provided by the Contractor.
Service Order Response	Number of Federal Government Working Days from the date of issuance of the Service Order to the Contractor until acceptance of the Work by the Technical Authority for the service.
Service Portal	Means the service portal provided and managed by the Contractor including the provision of documentation.
Service Portal Availability	Percentage of time that the service portal is fully operational.
Service Project Plan	Means the service project plan prepared by the Contractor for each service project.
Service Releases	Means a release of the Software, which is designed to operate on designated combinations of computer hardware and operating systems. A new System Release typically will be indicated by the addition of one (1) to the first digit of the release number (e.g., v.2.X.X would be the next System Release after v.1.X.X).
Threat and Risk Assessment (TRA)	A structured process designed to identify risks and provide recommendations for risk mitigation through analysis of system / service critical assets, potential threat events / scenarios, and inherent vulnerabilities.
Threat Management Capacity	A single or a combination of physical or virtual devices, which can deliver all the Threat Management Services at an expected Wire Speed.
Threat Management Service	A security service, from the list below, that can be enabled on a Threat Management Capacity:

Term	Definition
	• Firewall • Intrusion Detection & Prevention • Content Filtering • Anti-Virus • Anti-Spam • Data Loss Protection
Tunnel Mode	A configuration, which prevents a User Device from accessing a public network (e.g., the Internet) when a VPN Tunnel (remote LAN) is being used.
Upgrades	Means an update to the Licensed Software to add, extend, enhance and/or improve the existing features, functionality and/or performance of the program code, which is documented by a version or build number change to the right of the first decimal (e.g., Product X Version 1.0 changes to Product X Version 1.1 or Product X Version 1.0.0 changes to Product X Version 1.0.1), regardless of whether the Contractor refers to it as a "minor upgrade" or "major upgrade".
User	A person that uses the service.
User Device	An electronic device of a User that connects to the service.
Virtual Local Area Network (VLAN)	Logical network partition for a LAN.
Virtual Network (VN)	Logical network partition.
Virtual Route Forwarding (VRF)	Technology that allows multiple instances of a routing table to co-exist within the same router at the same time.
Virtual Traffic Rate (VTR)	Contracted Traffic Rate (CTR) assigned to a VN.
VPN Tunnel	A connection for transmitting data securely through an unsecured network such as the Internet. A VPN is "virtual" because it does not require dedicated lines. It is "private" because encryption is used to achieve security.
Vulnerability Assessment	The processes to determine the existence of system vulnerabilities.
Wireless Access Point	Wireless Access Point (WAP) is a device that allows wireless enabled Hosts to connect to a network using wireless network standards.
Wire Speed	When data is said to be transmitted at wire speed or at "wire rate," it implies there is little or no software overhead associated with the transmission and that the data travel at the maximum speed of the hardware.
Security Incident	A Security Incident is a type of Incident. It is a violation or imminent threat of violation of computer security policies,

Term	Definition
	acceptable use policies, or standard security practices that can or has the potential to cause negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malicious code that destroys data. Or An unauthorized behaviour (against the security policy of the IT system) regarding the operation and administration of the IT system that has the potential to compromise the IT systems confidentiality, integrity, or availability.

2 ACRONYMS

Acronym	Term
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AM	Ante Meridiem (Latin: before midday) the time interval from midnight to midday
ARL	Authority Revocation List
AS	Autonomous System
BGP	Border Gateway Protocol
CA	Certification Authority
CIR	Committed Information Rate
COTS	Commercial Off-The-Shelf
CRL	Certificate Revocation List
CSDD	Committed Service Delivery Date
CSEC	Communications Security Establishment Canada
CSV	Comma Separated Value
DOS	Denial of Service
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DNS	Domain Name System
DOS	Denial of Service
EAL	Evaluation Assurance Level
EIA	Electronic Industries Alliance
ERC	Enhanced Reliability Check
ESP	Encapsulation Security Payload
ET	Eastern Time (Canada)
FAX	Facsimile
FGWD	Federal Government Work Day
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol

Acronym	Term
FOCIS	Fiber Optic Connector Intermateability Standard
Gbps	Giga bits per second
GC	Government of Canada
GC.Net	Government of Canada Network
HTML	Hyper Text Mark-up Language
HTTP/HTTPS	Hypertext Transfer Protocol / Secure
ICD	Incident Control Document
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IEC	International Electro technical Commission
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IIS	Internet Interconnection Service
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITSB	Information Technology Services Branch
ITSG	Information Technology Security Guidance
LAN	Local Area Network
LDAP	Lightweight Directory access Protocol
LIAS	Local Internet Access Service
MAT	Monthly Average Throughput
MD	Message Digest
MRP	Monthly Recurring Price
MTTR	Mean Time to Repair
NAC	Network Access Control
NACR	Network Announcement Change Requests
NAP	Network Access Point
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System

Acronym	Term
NOC	Network Operations Centre
NRIC	Non-Recurring Installation Charge
OGD	Other Government Departments
ORP	Operational Readiness Plan
PAZ	Public Access Zone
PDL	Packet Data Loss
PTD	Packet Transit Delay
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
POS	Points of Service
PSTN	Public Switched Telephone Network
QOS	Quality of Service
RADB	Random Arbiter Data Base
RCA	Root Cause Analysis
RFC	Request For Comment
RPC	Remote Procedure Call
RPSL	Routing Policy Specification Language
SAN	SSC Authority Number
SSC	Shared Services Canada
SDI	Service Delivery Interval
SDP	Service Delivery Point
SIP	Service Interface Point
SLMP	Service Level Management Plan
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOCN	Service Order Completion Notice
SOA	Service Order Acceptance
SOR	Service Order Request
SOW	Statement of Work
SRA	Secure Remote Access
SRTM	Security Requirements Traceability Matrix
SSD	SSC Service Desk

Acronym	Term
SSL	Secure Sockets Layer
TA	Technical Authority
TBS	Treasury Board of Canada Secretariat
TCP	Transmission Control Protocol
Telnet	Protocol to connect remote terminals to a server over Internet
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TRA	Threat and Risk Assessment
TDD	Teletypewriter/Telecommunications Device for the Deaf
TTY	Teletypewriter
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Networks
VPN	Virtual Private Network
XML	Extensible Mark-up Language

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
10026415
Security Classification / Classification de sécurité Unclassified

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Shared Services Canada	2. Branch or Directorate / Direction générale ou Direction: Transformation and Services Strategy Design
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Internet Interconnect Services (IIS), to replace diverse and redudant Internet services under the expiring SCNet contracts.

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

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

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

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

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
10026415
Security Classification / Classification de sécurité Unclassified

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

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

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

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

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

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

☑ RELIABILITY STATUS COTE DE FIABILITÉ	☐ CONFIDENTIAL CONFIDENTIEL	☐ SECRET SECRET	☐ TOP SECRET TRÈS SECRET
☐ TOP SECRET– SIGINT TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL NATO CONFIDENTIEL	☐ NATO SECRET NATO SECRET	☐ COSMIC TOP SECRET COSMIC TRÈS SECRET
☐ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

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

10. b) May unscreened personnel be used for portions of the work? — No / Non ☑ Yes / Oui ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — No / Non ☐ Yes / Oui ☐
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
10026415
Security Classification / Classification de sécurité
Unclassified

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

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

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

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

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