Annex A: Statement of Work

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

Date: 06 May 2013

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 SIPs fail.

(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.

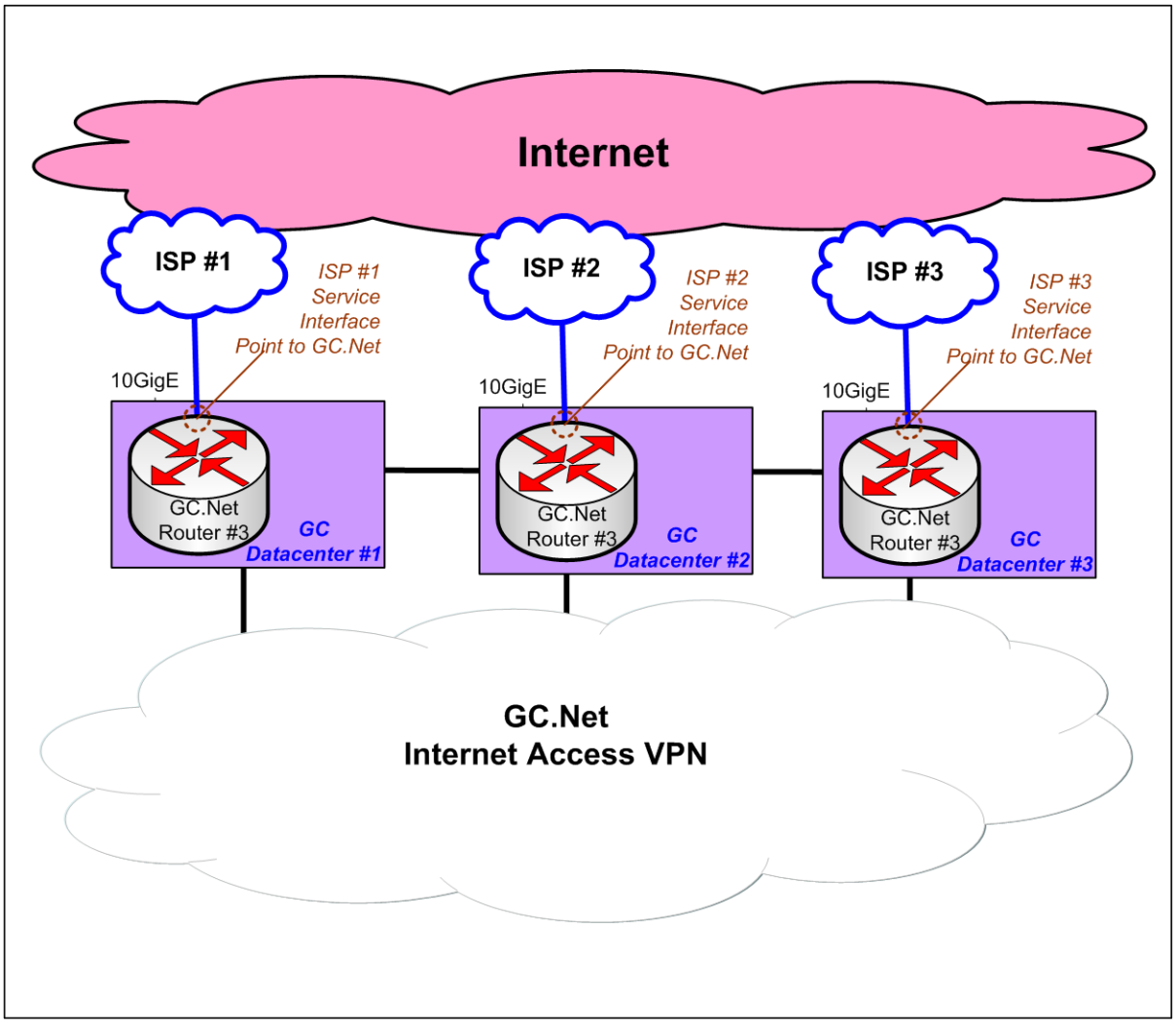

Figure 1: GC.NET Internet Infrastructure

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.

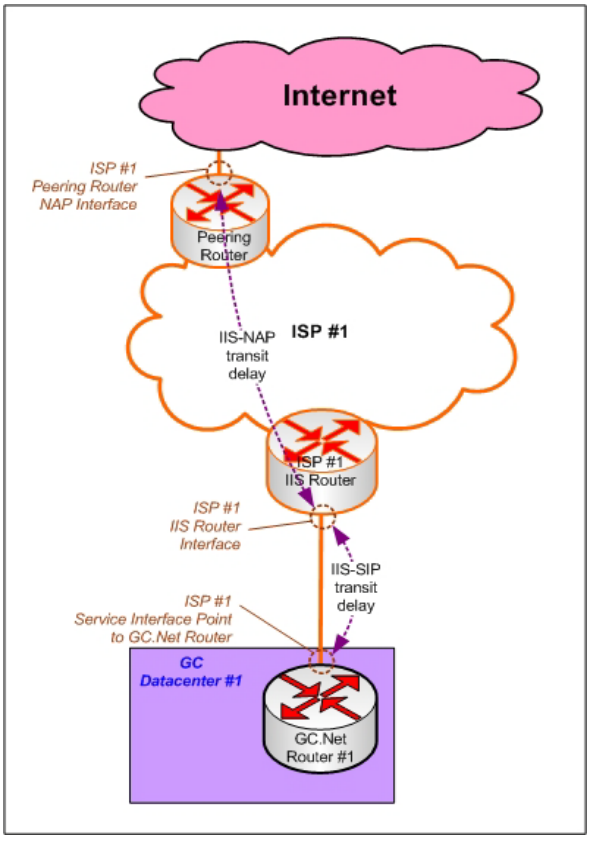

Figure 2 IIS-NAP transit delay and IIS-SIP transit delay

(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.

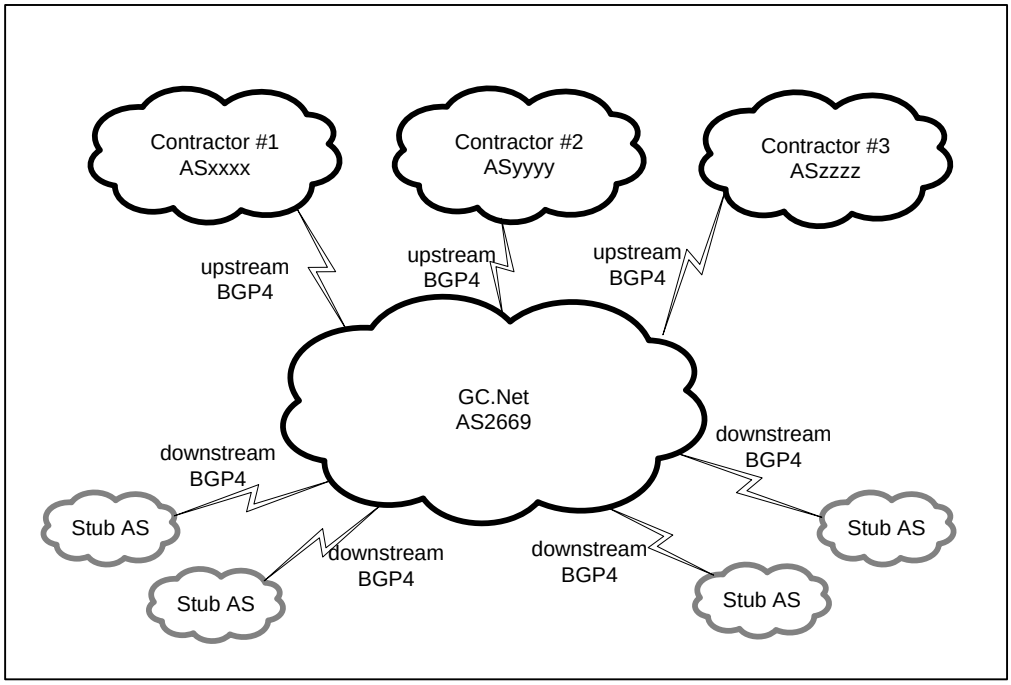

Figure 3: GC.Net Autonomous Systems

(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 5.3, 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;
   ii) Vulnerability Assessment Plan;
   iii) Security Installation Verification Plan;
   iv) Integration Security Test Report;
   v) Vulnerability Assessment Report, and
   vi) Security Installation Verification 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 Security Assessment and Authorization of the Installation

(134) The Contractor must provide SSC with a draft version of the following deliverables within 65 Federal Government Working Days after Contract award for approval by SSC:

a) integration security test plan (see Integration Security Test Plan subsection);
b) vulnerability assessment plan (see Vulnerability Assessment Plan subsection);
c) security installation verification plan (see Security Installation Verification Plan subsection);
d) integration security test report (see Integration Security Test Report subsection);
e) vulnerability assessment report (see Vulnerability Assessment Report subsection); and
f) security installation verification report (see Security Installation Verification Report subsection).

(135) The Contractor must wait for Gate 3 approval by SSC before declaring IIS ready for Use.

3.6.3.2 Integration Security Test Plan

(136) The Contractor must develop an Integration Security Test Plan that addresses integrated security functions.

(137) The Integration Security Test Plan must identify the tests to be performed and describe the scenarios for performing each test. Test scenarios must include any ordering dependencies on the results of other tests.

(138) The Contractor must include in the Integration Security Test Plan provisions for Canada representatives to witness the integration security testing.

(139) The Contractor must provide SSC with an Integration Security Test Plan that contains, at minimum, the following information:

a) the security functions to be tested;
b) Canada witnessing arrangements;
c) For each security function or sets of security functions, the items to be tested including:
    i) A description of the test case, procedure, or scenario;
    ii) Environmental requirements;
    iii) Ordering dependencies; and
    iv) Expected results (i.e., pass/fail criteria)

(140) The Contractor must provide SSC with an updated security requirements traceability matrix that contains, for each security requirement to be tested by the integration security test plan, the following information:

a) Tracing (a reference to an identifiable element) to integration security testing test cases.

3.6.3.3 Vulnerability Assessment Plan

(141) The Contractor must provide SSC with a Vulnerability Assessment Plan that contains, at minimum, the following information:

a) A description of the scope of the vulnerability assessment;
b) Canada witnessing arrangements;
c) A description of the vulnerability assessment process; and
d) A description of the vulnerability assessment tools that will be used, including any software versions.

3.6.3.4 Security Installation Verification Plan

(142) The Contractor must develop a Security Installation Verification Plan to conduct a comprehensive verification of the installation of security solutions and the security configuration of the IIS production environment.

(143) The Security Installation Verification Plan must identify the verifications to be performed and describe the scenario for performing each verification.

(144) The Contractor must include in the Security Installation Verification Plan provisions for Canada representatives to witness security installation verification.

(145) The Contractor must provide SSC with a Security Installation Verification Plan that contains, at minimum, the following information:

a) the security verification approach;
b) Canada witnessing arrangements;
c) an outline of the security verification items;
d) for each security verification item:
    i) a description of the verification scenario;
    ii) ordering dependencies; and
    iii) expected results (i.e., pass/fail criteria).

(146) The Contractor must provide SSC with an updated security requirements traceability matrix that contains, for each security requirement to be tested by the security installation verification plan, the following information:

a) tracing (a reference to an identifiable element) to security installation verification test

cases.

3.6.3.5 Integration Security Test Report

(147) The Contractor must conduct integration security testing in accordance with the Integration Security Test Plan.

(148) The Contractor must provide SSC with an Integration Security Test Report that contains, at minimum, the following information for each of the test items in the Integration Security Test Plan:

a) the expected results (i.e., pass/fail criteria);
b) the actual results; and
c) a description of deviations and how each was resolved.

3.6.3.6 Vulnerability Assessment Report

(149) The Contractor must conduct a vulnerability assessment in accordance with the Vulnerability Assessment Plan.

(150) The Contractor must implement patches and corrective measures as part of this activity. Where this is not feasible (e.g., time to test patch or determine and test corrective measures would seriously delay the project), the Contractor must create change management tickets for any required patch or corrective measure that cannot be implemented as part of the vulnerability assessment activity. These tickets are to be created in the change management system for the production environment for implementation during the in-service phase of the contract.

(151) The Contractor must provide SSC with a Vulnerability Assessment Report that contains, at minimum, the following information:

a) a listing of the vulnerability assessment tests that were conducted; and
b) for each vulnerability assessment test:
    i) whether a known vulnerability was detected;
    ii) a description of the vulnerability;
    iii) a description of the patch or corrective measure that was implemented to resolve the vulnerability; and
c) for any unresolved vulnerability:
    i) an assessment of the significance of the vulnerability in the context of the SSC IIS Services;
    ii) the problem ticket number for the outstanding patch or corrective measure; or
    iii) the rationale for not implementing a patch or a corrective measure.

3.6.3.7 Security Installation Verification Report

(152) The Contractor must conduct security installation verification in accordance with the Security Installation Verification Plan.

(153) The Contractor must correct installation and configuration errors and omissions that are detected as a result of the security installation verification.

(154) The Contractor must provide SSC with a security installation verification report that contains, at minimum, the following information for each of the test items in the security installation verification plan:

a) the expected results (i.e., pass/fail criteria);
b) the actual results; and
c) a description of deviations and how each was resolved.

3.6.4 Security Concept of Operations

(155) 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

(156) 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

(157) 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

(158) 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

(159) 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

(160) 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.

(161) 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

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

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

(164) 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/);

(165) 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.

(166) 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

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

(168) 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

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

(169.a) Preliminary Design,

(169.b) Critical Design, and

(169.c) Operational Readiness Review.

3.7.2.1 Preliminary Design

(170) 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.

(171) 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.

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

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

3.7.2.2 Critical Design

(174) 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).

(175) 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.

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

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

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

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

(180) 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.

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

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

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

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

3.7.2.3 Operational Readiness Review

(185) 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.

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

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

(188) 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:

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

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

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

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

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

(189) 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.

(190) 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

(191) 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.

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

3.7.4 Network Connectivity

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

4 SERVICE MANAGEMENT

(194) 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.

(195) 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.

(196) 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.

(197) 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

(198) 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.

(199) 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.

(200) 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.

(201) 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.

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

(203) 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

(204) 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.

(205) 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.

(206) 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

(207) 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.

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

(209) 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.

(210) 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.

(211) 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.

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

(213) The Contractor must provide support, on a 24/7/365 basis, to receive calls from SSC regarding service affecting issues.

(214) 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.

(215) The Contractor must notify SSC within 15 minutes of any service affecting issues detected or reported.

(216) The Contractor must track, monitor and report all service affecting issues.

(217) 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.

(218) 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.

(219) The Contractor must attend meetings, to discuss and resolve issues regarding the performance of the services.

(220) When requested, Contractor's technical experts must attend the meeting.

(221) 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

(222) 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.

(223) 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.

(224) The Contractor must provide notification and work details, and must obtain approval from SSC 10 FGWDs in advance of the work to be done.

(225) The Contractor must coordinate new and additional installs, upgrades, and configuration and repairs of Services with SSC by:

(225.a) Calling before the actual start of work and identifying technician(s) performing the work;

(225.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;

(225.c) Calling to confirm completion of work and restoration of service; and,

(225.d) Submitting email notification of the description and completion status of the work to the Technical Authority.

(226) The Contractor must monitor and report all incidents on a 24/7/365 basis on the services provided to SSC.

(227) The Contractor must provide support on a 24/7/365 basis to receive calls from SSC regarding service issues.

(228) The Contractor must work cooperatively with SSC and other IIS Contractor, to resolve service incidents and problems.

(229) The Contractor must notify by email or phone to SSC within 15 minutes of any service problems detected or incidents reported.

(230) The Contractor must use a trouble ticketing system to track, monitor and report all service incidents and problems.

(231) 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.

(232) 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.

(233) 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.

(234) 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

(235) 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.

(236) 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.

(237) 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.

(238) The Contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this audit.

(239) 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.

(240) 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.

(241) 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.

(242) 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

(243) The Contractor must provide all components required to perform Management Services for the IIS, at no additional cost to SSC.

(244) The Contractor must provide Management Services for the IIS at no additional cost to SSC.

(245) 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.

(246) 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.

(247) The Contractor must provide notification and obtain approval from SSC 10 FGWDs in advance of the work to be done.

(248) 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

(249) 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.

(250) All Change Requests must be approved by SSC.

(251) 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.

(252) The Contractor must create at least 1 Change Ticket for each Change Request submitted by SSC within 1 FGWD of receiving the Change Request.

(253) 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.

(254) The Contractor must implement Change Requests, excluding Emergency Changes, during maintenance windows as approved by SSC.

(255) The Contractor must escalate Change Requests as requested by SSC.

(256) 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.

(257) The Contractor must revise the contents of the Change Ticket information fields or change acceptance test plan as requested by SSC.

(258) 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).

(259) 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.

(260) 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.

(261) 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.

(262) 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.

(263) The Contractor must provide a Change Request Cancellation Notice to SSC, within 24 hours of cancellation of the Change Request by the Contractor.

(264) 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.

(265) The Contractor must provide acceptance-testing results in the Change Ticket, within 2 FGWDs after the completion of a Change Request.

(266) The Contractor must successfully complete the Acceptance Test Plan in the Change Ticket before the Change Request is accepted by SSC.

(267) The Contractor must close the Change Tickets for a Change Request after the Change Request has been accepted by SSC.

(268) The Contractor must provide a Change Request Completion Notice to SSC within 2 FGWDs of the completion of any Change Request.

(269) 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

(270) 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

(271) 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.

(272) 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.

(273) The Contractor must escalate incidents, if an incident has remained open, based on clear and well-established escalation levels, procedures and processes.

(274) 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.

(275) The Contractor must provide SSC with notification of incidents according to the operational and management escalation matrices.

(276) The Contractor must change the Escalation Level for incidents within 15 minutes of a request by SSC.

(277) The Contractor must create an incident ticket for each incident.

(278) The Contractor must log all privacy or security violations and other security related events as incidents.

(279) 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.

(280) 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).

(281) The Contractor must open an incident ticket within 5 minutes for both Contractor-determined and SSC-reported incidents.

(282) The Contractor must update the incident ticket information log following a change in status.

(283) The Contractor must document all management and technical escalations for incidents in the incident ticket information log.

(284) 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.

(285) The Contractor must track and report the outage time of each incident in the associated Incident Tickets.

(286) 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.

(287) 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.

(288) The Contractor must suspend an incident (Incident Ticket resolution outage timer placed on hold) at SSC's request.

(289) An incident suspended by SSC must remain suspended until released by SSC or for a fixed time period specified by SSC.

(290) 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.

(291) 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.

(292) 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.

(293) 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.

(294) The Contractor must obtain SSC's approval before closing an incident.

(295) The Contractor must close the Incident Tickets after SSC has approved closing the Incident.

(296) The Contractor must notify SSC of the resolution of an incident according to severity as specified by SSC.

(297) 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.

(298) The Contractor must identify and document the causal factors (root causes) of all Incidents.

(299) The Contractor must develop workarounds to address all identified root causes.

(300) The Contractor must designate 3 or more Incidents with the same root cause within a rolling 90-day window as a Chronic Problem.

(301) The Contractor must assign the next highest severity for Incidents designated as chronic problems.

(302) The Contractor must link Incidents to existing or new Chronic Problems as requested by SSC.

(303) 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

(304) 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.

(305) The Contractor must provide release notes for any IIS release within 40 FGWDs prior to the implementation of the release.

(306) The Contractor must not implement any releases for the IIS without prior approval from SSC.

(307) 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

(308) 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

(309) The Contractor IIS must respond to any failure situation to ensure Internet access availability.

(310) 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.

(311) 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.

(312) The Contractor must notify SSC of scheduled outages of the IIS at least 20 FGWDs in advance of a scheduled outage.

(313) The Contractor must obtain SSC's approval for any scheduled outages of the IIS.

6 MEETINGS

(314) 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.

(315) 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.

(316) 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.

(317) 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.

(318) 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.

(319) 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.

(320) The Contractor must organize and participate in weekly meetings to review new and outstanding SORs.

(321) 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

(322) The Contractor must provide all required documents and reports identified in this SOW, including the documents listed and described in this Section.

(323) The Contractor must provide all IIS documentation and reports in English and COTS file format approved by SSC.

(324) The Contractor must post reports electronically in the respective EIET for access and download by authorized persons as specified by SSC

(325) The Contractor must track versions and change history for changes to IIS reports and documentation.

(326) 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.

(327) The Contractor must not require the use of ActiveX components for access to IIS reports and documentation.

(328) Unless otherwise indicated for a specific report in the SOW, the Contractor must provide monthly reports 5 FGWDs following the previous reporting month.

(329) The Contractor is responsible for maintaining the information accuracy and delivering updated documentation within 5 FGWDs of any changes or updates to SSC.

(330) 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.

(331) 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.

(332) 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

(333) 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.

(334) 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.

(335) The Contractor must provide a monthly Financial Expenditure report to SSC.

7.2 Reports by Special Request

(336) 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.

(337) 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.

(338) 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.

(339) 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

(340) 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.

(341) 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

(342) 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.

(343) 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.

(344) 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.

(345) The IIS Configuration Document must, at a minimum, contain the following information:

(345.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;

(345.b) Telecommunications facility capacity along with the performance thresholds for high availability and diversity requirements;

(345.c) The configuration of the interface of the Contractor's IIS Router, with passwords being deleted;

(345.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;

(345.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;

(345.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);

(345.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,

(345.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.

(346) The Contractor must maintain information accuracy and update their respective IIS Configuration Document for the life of the Contract.

(347) The Contractor must deliver the updated documentation within 5 FGWDs of any changes or updates.

(348) Any revision of the IIS Configuration Document is subject to approval by SSC.

8 MANAGEMENT REPORTING

8.1 Electronics Information Exchange Tool (EIET)

(349) 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.

(350) The Contractor must make the EIET available for use within 60 FGWD days of Contract award.

(351) 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.

(352) The Contractor must protect the confidentiality of hosted information by restricting access to only authorized persons approved by SSC.

(353) If the Contractor’s approved EIET is a Web Portal or other equivalent application:

(353.a) The Contractor must create and manage user accounts for individuals authorized by SSC when requested.

(353.b) The EIET must log all access automatically and the Contractor must provide the access logs to SSC when requested.

(353.c) The Contractor’s EIET must enforce the following password requirements for user log in:

(353.c.1) Contain at least 6 characters;

(353.c.2) Change required every 60 days; and

(353.c.3) Contain upper and lower characters with at least 1 numerical symbol.

(353.d) The Contractor must lock down access to the EIET by IP addresses and application port numbers.

(353.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).

(354) 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.

(355) The Contractor may request deviations from this design or propose an alternate security perimeter design but are subject to approval by SSC.

(356) The Contractor must provide an EIET that will allow SSC to execute, view and download reports.

(357) The Contractor must provide reports available in HTML, CSV and XML formats or other formats approved by SSC.

(358) The Contractor must provide SSC with the ability to configure and define reports, based on the information system provided.

(359) The Contractor must allow SSC the option to enable mitigation or disable mitigation against a Denial of Service (DOS) event on the EIET.

(360) 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 5.1.

8.2 IP Traffic Data

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

(362) 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.

(363) 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.

(364) 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.

(365) 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

(366) The Contractor must provide reports on the Anti-Distributed Denial of Service that will:

(366.a) Be available in HTML, XML, CSV and XML formats or other formats approved by SSC.

(366.b) Be automatically sent on a periodic basis to specific email addresses provided by SSC.

(366.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.

(366.d) Showing the top 100 addresses consuming the most bandwidth as a Top Talker Summary Report.

(366.e) Show information about the worms and infected hosts in the network as a Worm Activity Report.

(366.f) Show information on the scrubbing of IP traffic as a Threat Mitigation Report.

(366.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

(367) The communications between the Contractor and SSC must be coordinated and flow through Canada.

(368) 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.

(369) The Contractor's Operations Management Procedures must describe in detail the respective Contractor's processes and procedures regarding service operations and delivery to SSC.

(370) 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

(370.a.1) Trouble ticketing system and processes,

(370.a.2) Incident handling flowchart,

(370.a.3) Incident Reporting and Notification Escalation Procedures,

(370.a.4) Resolution times, and

(370.a.5) Root Cause Analysis.

8.4.2 Contractor's Helpdesk and Support Organization

(370.a.6) 24 /7/365 access and support, and

(370.a.7) Helpdesk telephone and e-mail contact information

8.4.3 Change Management Procedures and System

(370.a.8) Handling of Types of Changes (Emergency, Maintenance, Release),

(370.a.9) Flowchart of ordering and provisioning process, and

(370.a.10) Turnaround timeframes.

8.4.4 Security Management Procedures

(370.a.11) Contractor's Corporate Security Policy,

(370.a.12) Security Control Systems, and

(370.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:

(370.b) A list of the service measurements reported for each service;

(370.c) The method and frequency used for service measurements;

(370.d) Calculations used to derive reported Service Level values;

(370.e) A summary of Service Level Report formats used; and

(370.f) Service Level Objectives and Guarantees (if applicable) for each service.

8.6 Service Level Reports

(371) 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.

(372) The Contractor must post the Service Level Reports in electronic format on their EIET. The reports must include:

(372.a) The Contractor's service performance values;

(372.b) Trouble ticket report of service incidents and problems, describing the incident, issues, diagnosis, corrective actions and resolution time; and,

(372.c) Order provisioning report that provides the description, date started, and date completed of the orders in progress and completed.

(373) 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

(374) The Contractor must provide the capability to process and track Service Order Requests through the EIET.

8.8 Interface Control Document (ICD)

(375) The Contractor must provide ICD documents that contain the service information of the technical interface between the Contractor IIS and SSC Intranets.

(376) 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.

(377) The Contractor must provide the following information in their ICD:

(377.a) Contractor's contact information;

(377.b) A description of the physical layer of the IIS;

(377.c) A description of the data link layer of the IIS including data link encapsulation protocols and settings;

(378) The Contractor must ensure that its input into the ICD is accurate and current;

(379) The Contractor must provide changes or updates to the ICD within 3 FGWDs; and

(380) The revised ICD will be re-issued by the Contractor and provided to SSC for review by the Contractor.

8.9 Security

(381) 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.

(382) 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.

(383) 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.

(384) 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.

(385) 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:

(386) 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.

(387) 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

(388) 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.

(389) The Contractor must provide supporting evidence within 10 FGWDs of a request by SSC for any supporting evidence required for the conformance review.

(390) 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

(391) 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.

(392) The Contractor must take the necessary measures on its interfacing equipment or infrastructure to maintain service levels.

(393) 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.

(394) The Contractor must monitor and measure service levels 24 hours per day, 7 days per week, and 365 days per year.

(395) The Contractor must provide any hardware and/or software that are necessary to monitor and measure service levels.

(396) The Contractor must calculate and report service levels to two decimal points, unless otherwise indicated for a service level.

(397) 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.

(398) 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.

(399) The "availability" is a percentage function based on the cumulative outage periods and the total time the IIS is available as follows:

$$\frac{\text{(Expected Service Availability for the Month – Cumulative Outage for the Month)}}{\text{Expected Service Availability for month}} \times 100\%$$

(400) 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)

(401) 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)

(402) 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.

(403) 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:

(404) 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)

(405) The SL-MTRS for the IIS the Anti-DDoS is within 4 hours.

(406) 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.

(407) 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)

(408) 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)