Procurement and Contracting Services
30 Victoria Street, Gatineau QC K1A 0M6

Supplier@elections.ca

REQUEST FOR INFORMATION

Office of the Chief Electoral Officer File No.:
ECBR-RFI-17-0001

Title:	**Date:**
Metropolitan Area Network and Wide Area Network Services	August 14, 2017
Closing Date and Time:	
August 28, 2017 at 2:00 p.m. (Gatineau time)	

ENQUIRIES	
Address enquiries to:	
Supplier@elections.ca	
Attention:	**Tel No.**
Barbara D. Robertson	819-939-1493

RESPONSES
Submit responses to:
Supplier@elections.ca

This Request for Information ("RFI") contains the following information:

Annexes

REQUEST FOR INFORMATION

Metropolitan Area Network and Wide Area Network Services

PART 1. Background and Purpose

1.1. Purpose

In order to assist Elections Canada (EC) in refining its requirements, EC is seeking feedback from suppliers regarding its requirement for Metropolitan Area Network and Wide Area Network Services.

Elections Canada is issuing this RFI to validate solution concepts that could assist EC in further defining requirements and refine the procurement strategy, requirements definition and other aspects of the requirement.

1.2. EC Mandate

EC, headed by the Chief Electoral Officer (CEO), an agent of Parliament, is an independent, non-partisan agency with unique organizational features that reports directly to Parliament. EC exercises general direction and supervision over the conduct of election events such as general elections, by-elections and referendums at the federal level. Its mandate is to:

a) be prepared to conduct a federal general election, by-election or referendum;

b) administer the political financing provisions of the Canada Elections Act (CEA);

c) monitor compliance with electoral legislation;

d) conduct public information campaigns on voter registration, voting and becoming a candidate;

e) conduct education programs for students on the electoral process;

f) provide support to the independent commissions in charge of adjusting the boundaries of federal electoral districts following each decennial census;

g) carry out studies on alternative voting methods and, with the approval of parliamentarians, test alternative voting processes for future use during electoral events; and

h) provide assistance and cooperation in electoral matters to electoral agencies in other countries or to international organizations.

1.3. Project Description

EC requires a Contractor to provide on-going MAN/WAN network services to EC. Currently, EC is considering that a portion of these services will be unmanaged Layer 2 MAN while the remaining services will be managed MPLS.

1.4. Anticipated Procurement Timeline

EC is at the preliminary stage of the procurement process. The high-level procurement timeline will follow a multi-phase procurement process that will likely include the following key activities:

Procurement Phase	Estimated Timeline
Planning – RFI	August 2017
Solicitation	September - October 2017
Evaluation	November 2017
Contract Award	November 2017

PART 2. Nature of Request for Information

This is not a solicitation of bids or proposals. This RFI may not lead to the launching of a procurement process, the award of any contract or the creation of a source list. As a result, suppliers of any goods or services described in this RFI should not reserve stock or facilities, nor allocate resources, as a result of any information contained in this RFI. Therefore, whether or not any supplier responds to this RFI, it will not preclude that supplier from participating in any future procurement. Also, the decision to whether or not to launch a procurement process for any of the goods or services described in this RFI is entirely at the sole discretion of EC. EC reserves the right to cancel or modify any of the preliminary requirements described herein. This RFI is simply intended to solicit feedback from industry with respect to the matters described herein and should not be considered as an authorization to undertake any work that would result in costs being charged to EC. EC reserves the right to accept or reject any or all comments received. Further respondent engagement may be conducted by EC which may include supplier engagement days, one-on-one meetings, product demonstrations, requesting additional information from respondents, etc.

PART 3. Nature and Format of Responses Requested

Respondents are invited to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this RFI could be satisfied. Respondents are also invited to provide comments regarding the content, format and/or organization of any draft documents included in this RFI. Respondents should explain any assumptions they make in their responses.

PART 4. Response Costs

EC will not reimburse any respondent for any expenses or costs incurred in responding to this RFI.

PART 5. Treatment of Responses

5.1. Use of Responses

Responses will not be formally evaluated. However, the responses received may be used by EC to develop or modify procurement strategies or any draft documents contained in this RFI. EC will review all responses received by the RFI closing date. EC may, in its discretion, review responses received after the RFI closing date.

5.2. Review Team

A review team composed of representatives from EC will review the responses. EC reserves the right to hire any independent consultant, or use any government resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

5.3. Confidentiality

Respondents are solely responsible for marking any portions of their response that they consider proprietary or confidential. EC will handle the responses in accordance with the *Access to Information Act* and the *Privacy Act*

5.4. Follow-Up Activity

EC may, at its discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response or for one-on-one meetings.

PART 6. Official Languages

Responses to this RFI may be submitted in either of the official languages of Canada, French or English.

PART 7. Information Requested by Elections Canada

7.1. Comments on Preliminary Documents

Attached to this RFI are the following documents for which EC is seeking comments from industry:

a) Annex A – Draft Statement of Work

b) Appendix A to Annex A – Draft Glossary of Terms and Acronyms

c) Appendix B to Annex A – Statement of Work Security Requirements

d) Appendix C to Annex A – Service Classes

These documents are currently at a preliminary stage only and new clauses or requirements may be added at EC's sole discretion to any solicitation that may ultimately be published by EC.

Any of the clauses or requirements may be deleted or revised if used in any procurement process, at EC's sole discretion. Comments regarding any aspect of the draft document are welcome.

7.2. Responses to Questions to Industry

EC requests responses to the questions found in Annex B – Questions to Industry.

PART 8. Format of Responses

8.1. Cover Page

If the response includes multiple volumes, respondents should indicate on the front cover page of the response the title of the response, the RFI number, and the number of volumes and the full legal name of the respondent.

8.2. Title Page

The first page of each volume of the response should be the title page, which should contain:

a) the title of the respondent's response and the volume number;

b) the name and address of the respondent;

c) the name, address, telephone number and email address of the respondent's contact;

d) the date; and

e) the RFI number.

8.3. Numbering System

Respondents should prepare their response using a numbering system corresponding to the one in this RFI. All references to descriptive material, technical manuals and brochures included as part of the response should be referenced accordingly.

PART 9. Enquiries

This is not a solicitation, therefore EC will not necessarily respond to enquiries in writing or by circulating answers to all potential respondents. However, respondents with questions regarding this RFI may direct their enquiries to the Contracting Authority via the email address identified on the cover page of this document.

PART 10. Submission of Responses

10.1. Time and Place for Submission of Responses

Respondents interested in providing a response should submit it by email to the Contracting Authority via the email address and by the closing date and time identified on the cover page of this document.

10.2. Responsibility for Timely Delivery

Each respondent is solely responsible for ensuring its response is delivered on time to the correct location.

10.3. Identification of Response

Each respondent should ensure that its name, contact person and email address, the RFI number and the closing date are included in their response in a prominent location.

Metropolitan Area Network and Wide Area Network Services

Statement of Work (SOW)

(Draft)

Table of Contents

PART I – INTERPRETATION

1. Appendices

The following appendices are attached to and form an integral part of this SOW:

a) Appendix A – Glossary of Terms and Acronyms

b) Appendix B – Service Classes

c) Appendix C – Statement of Work Security Requirements

2. EC Mandate

EC, headed by the CEO, an agent of Parliament, is an independent, non-partisan agency with unique organizational features that reports directly to Parliament. EC exercises general direction and supervision over the conduct of elections and referendums at the federal level. Its mandate is to:

a) be prepared to conduct a federal general election, by-election or referendum;

b) administer the political financing provisions of the CEA;

c) monitor compliance with electoral legislation;

d) conduct public information campaigns on voter registration, voting and becoming a candidate;

e) conduct education programs for students on the electoral process;

f) provide support to the independent commissions in charge of adjusting the boundaries of federal electoral districts following each decennial census;

g) carry out studies on alternative voting methods and, with the approval of parliamentarians, test alternative voting processes for future use during electoral events; and

h) provide assistance and cooperation in electoral matters to electoral agencies in other countries or to international organizations.

3. Objective

EC requires a Contractor to provide on-going MAN/WAN network services to Elections Canada. A portion of these services will be unmanaged, as further described in Part II, while the remaining services will be managed, as further described in Part III.

4. Overview of Network Services

4.1. Current EC Metropolitan Area Network/Wide Area Network Services

4.1.1. This subsection, Current EC Metropolitan Area Network/Wide Area Network Services, provides a description of current EC MAN/WAN Services provisioned through various EC and SSC contracts. At the time of writing, this is the current configuration of EC MAN/WAN Services; however, this configuration is subject to change.

4.1.2. EC has high-speed MAN services between buildings in the NCR. The current topology consists of a star topology with the EC King Edward Datacentre (KED) acting as the hub and other locations, listed below, as edge nodes in a Layer 2 unmanaged MAN.

a) 30 Victoria

b) 150 Tunney's Pasture

c) 440 Coventry

4.1.3. Figure 1 below depicts the existing MAN configuration.

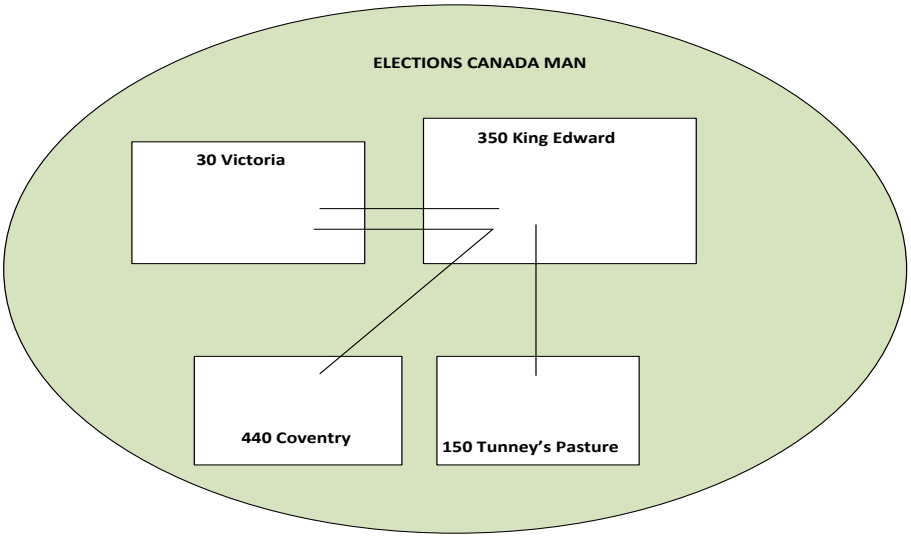

Figure 1: Elections Canada Logical MAN

4.1.4. In addition to the MAN links described above, the EC WAN also includes the links specified below:

a) a primary 80 megabits per second (Mbps) link to SSC (SMS) for Internet access

b) a secondary 5 Mbps link to SSC (SMS) for Internet access

c) dual 50 Mbps MPLS links to a Bell datacentre at 8100 Warden Avenue in Markham, Ontario

d) hundreds of Internet-based IPSec VPNs to connect field offices over public wireless services (3G/LTE) and Digital Subscriber Line services

4.1.5. The current networking and operational environments at 30 Victoria and KED have grown organically over several years. They have successfully served to deliver numerous Electoral Events including the 42nd general election. The legacy systems, servers and WAN demarcation are housed at KED providing the core of EC MAN/WAN Services. The MAN/WAN current environments are provided by Rogers Fibre MAN services and by Virtual Route and Forwarding (VRF) services in the Bell Multiprotocol Label Switching (MPLS) cloud.

4.1.6. 30 Victoria houses two Cisco 6509E that are connected over two diverse circuits to two 6509E Cisco core switches at KED providing a redundant virtual switching service configuration. These links provide an aggregate of two Gbps active-active connectivity between ECHQ and the network core at KED. Each EC telecom closet at 30 Victoria has two 3750 Cisco access switches for redundancy (six switches per floor). Floors 1, 9, 10, 11, 12 and 13 use Cisco 3750 switches to supply Local Area Network (LAN) connectivity for end-user devices and network services such as Power over Ethernet (PoE), which are required to support any unified communication, VoIP or wireless network infrastructure.

4.2. Anticipated MAN/WAN Requirements

4.2.1. During the term of the Contract it is possible that there will be additional buildings used by EC requiring additional network segments or that the number of required buildings will decrease, resulting in a reduction in network requirements.

4.2.2. Bandwidth requirements may also increase due to new applications or other unforeseen requirements.

4.2.3. EC's desired end state is a managed MPLS based MAN/WAN infrastructure; therefore EC requires the ability to buy managed MPLS services as and when requested. EC is envisioning an operating environment with multiple Software as a Service (SaaS) implementations, new Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) providers, outsourced contact centres and possibly other business locations. The exact address of these services is not known at this time; however all additional service locations will be located in Canada. As such, EC will require the ability to expand its network to handle solution integration.

4.2.4. Figure 2 shows a representative future solution architecture. The diagram depicts shaded areas where MPLS connectivity may be required in the future for SaaS and telephony services.

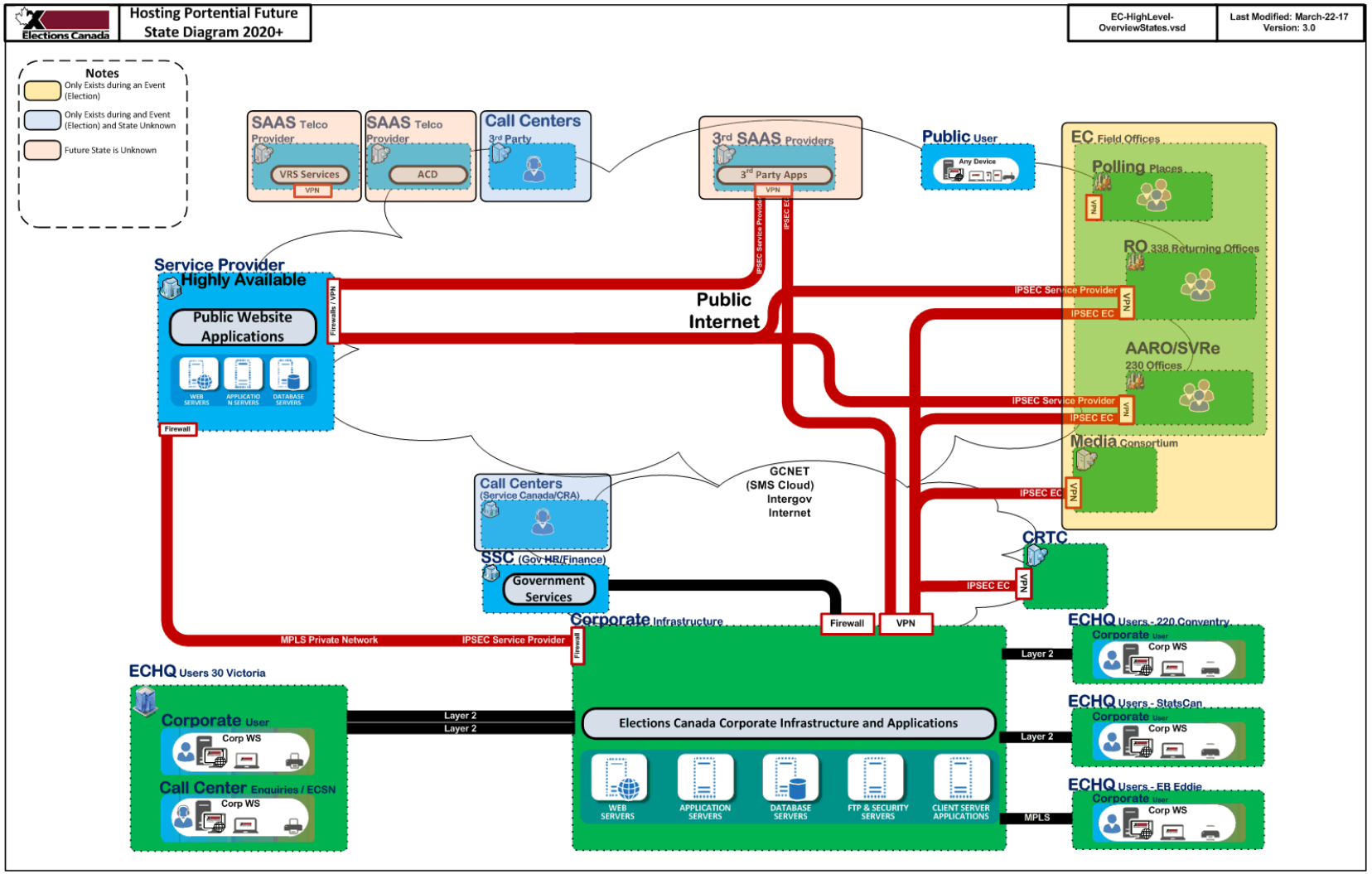

Figure 2: Possible Future Solution Architecture

PART II – UNMANAGED METROPOLITAN AREA NETWORK

5. Overview of Virtual Private Line Service Requirements to Remote Sites

5.1. King Edward Datacentre

The Contractor must provide VPLS Layer 2 service from the 30 Victoria CE aggregation service router to the KED CE aggregate service router. The Contractor must provide Ethernet Virtual Private Line (EVPL) dedicated point-to-multi-point type connections between 30 Victoria and KED and remote Layer 2 User Network Interface connections to 150 Tunney's Pasture and 440 Coventry. This standard Ethernet offering must deliver basic Ethernet service on a dedicated Ethernet port with the option to multiplex Ethernet Virtual Circuits (EVCs) to remote sites onto a dedicated Ethernet port. These EVCs must be handed off as 802.1q VLANs. EVC speeds are rate limited by bandwidth chosen as stipulated in the Services below at the ingress of both PE routers. Figure 3 below is an architecture overview of EC Ethernet Virtual Private Line Ethernet Services.

5.2. National Capital Region

Ethernet network services between EC facilities in the NCR are interconnected over a high-speed network in a hub-and-spoke configuration where the hub is KED. At the time of writing, only one link between 30 Victoria to KED will require diversity. The Contractor must maintain this configuration with new or existing network services.

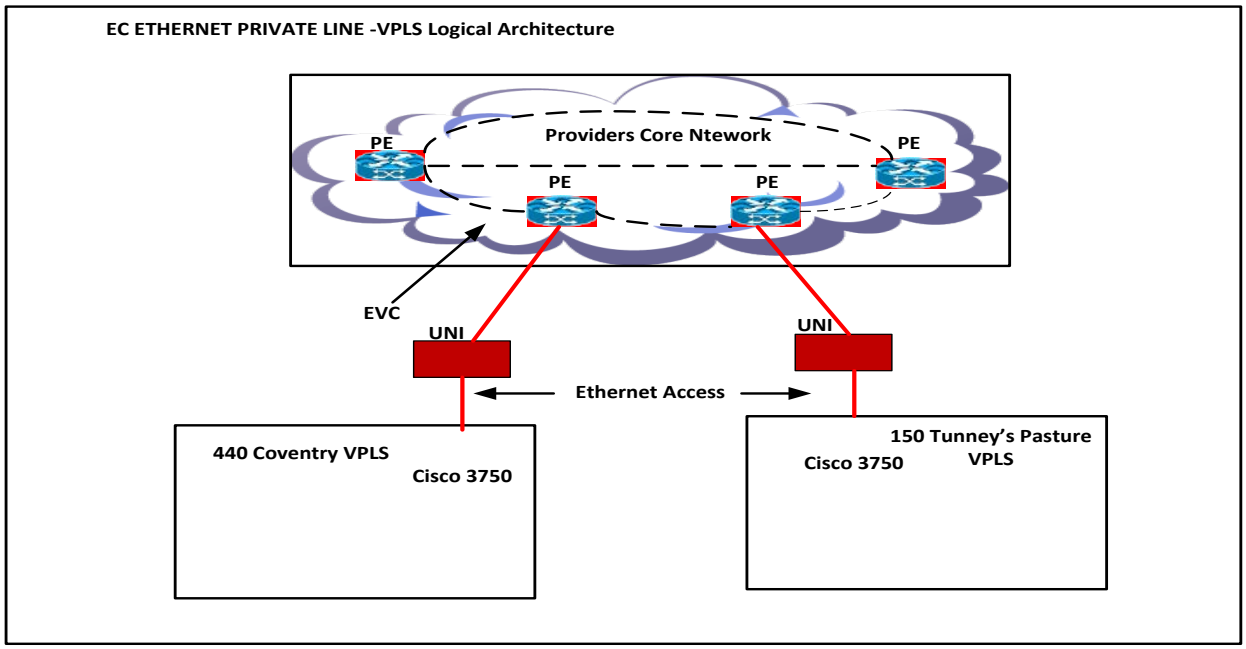

Figure 3: Ethernet Private Line Overview (EVPL-VPLS)

6. Layer 2 Network Services

6.1. Elections Canada Unmanaged Sites

As further stipulated below, the Contractor must provide connectivity, bandwidth and Layer 2 network services to the following locations:

Building	Dedicated Ethernet Bandwidth Required
440 Coventry	100 Mbps
150 Tunney's Pasture	100 Mbps
30 Victoria	2,000 Mbps (primary and diversity)
KED (or relocated building)	2,000 Mbps (primary, diversity and remote sites)

Table 1: EC Unmanaged Sites

6.2. Layer 2 Service Requirements

The Contractor must:

a) provide VPLS Layer 2 from 440 Coventry to KED as shown in Figure 2

b) provide VPLS Layer 2 from 150 Tunney's Pasture to KED as shown in Figure 2

c) apply labels to the PE routers only

d) employ an Request For Comment 1918 private addresses scheme or property registered American Registry for Internet Numbers (ARIN) public addresses

e) implement at minimum Secure Hash Algorithm (SHA) 2 or SHA-1 authentication

f) apply traffic shaping only to the ingress PE port onto the EVC

6.3. Elections Canada Virtual Local Area Networks

The Contractor must allow EC network management personnel and give them the ability to fully and transparently configure and manage the EC VLAN environment without requiring intervention from the Contractor.

6.4. Scaling

At the request of the Technical Authority through a Service Order, the Contractor must provide the following Layer 2 services:

a) bandwidth scaling at pre-established increments of 100 Mbps or 1,000 Mbps differentials within five business days

b) addition or removal of edge facilities

c) addition or removal of redundant links between facilities

6.5. Ethernet Standards

The Contractor must provide support for the following Ethernet network standards:

a) transparent Layer 2 and Layer 3 services

b) Layer 2 and 3 VLAN tags

c) Layer 2 and 3 control protocol:

   i. Spanning Tree Protocol (STP)

   ii. Cisco Discovery Protocol (CDP)

   iii. Link Layer Discovery Protocol (LLDP)

   iv. Link Aggregation Control Protocol (LACP)

d) Layer 3 routing protocols:

   i. Enhance Interior Gateway Routing Protocol (EIGRP)

   ii. Routing Information Protocol (RIP)

   iii. Open Shortest Path First (OSPF)

   iv. Multiprotocol Label Switching (MPLS)

   v. OpenFlow

   vi. Intermediate System to Intermediate System (ISIS)

e) Layer 3 Internet Protocol routing (IP version 4 and IP version6)

f) broadcast and multicast traffic at line rate

g) quality of service (803.1q)

h) VLAN transparent service, multi-stacking of 802.1q tags like QinQ, up to maximum transmission unit (MTU) size port speeds of 10/100/1,000 Mbps with bandwidth increments of 10/100/1,000 Mbps

i) traffic shaping

j) 802.1q tagging, 802.3 frames and 802.1ad/QinQ

k) 803.10 Base-T

l) 802.3U 100Base-TX, 100 Base-FX

m) 802.3Z 1000Base-X

n) 802.1P/Q VLAN multi-link tagging standard

o) must permit split multi-link trunking

p) multiple VLANs over one physical port

7. Provider Edge Router Services

7.1. Provider Edge Router Design

The Contractor must provide PE Router design configuration and implementation addressing the following elements:

a) hardware configuration including necessary parts and modules

b) IOS/software versions

c) Network access, routing, and IP addressing schemes

d) security parameters and policies

e) design testing

7.2. Provider Edge Router Implementation

7.2.1. The Contractor must configure and turn-up the PE router as part of any implementation plan required for maintaining and/or replacing the existing Layer 2 networking services. This must include the following elements:

a) Lead time for implementation at a particular EC site is dependent on site location, hardware availability, and network access type. The Contractor must provide EC with an implementation plan at the beginning implementation stage.

b) Certain pieces of hardware may be subject to manufacturing limitations or supply shortages, where there are unforeseen limitations or shortages on hardware supplied by the Contractor, and where it's financially viable. The Contractor must source the hardware from alternative suppliers. The Contractor must notify EC of changes to the implementation plan

7.2.2. Any implementation plan changes requested by EC must be approved by the Contractor and EC; changes will be documented in a revised implementation plan. EC must submit all change requests in writing to the Contractor's sales team.

8. Network Performance

8.1. Network Performance, Reliability and Stability Service Levels

The Contractor must meet the following service levels for performance, reliability and stability:

a) The packet error rate must be less than 0.1% over a period of one month.

b) The transmission delay (latency) must be less than 20 milliseconds on all received packets. The bandwidth provisioned at each site must accommodate a sustained bandwidth usage at the rated bandwidth in full duplex without dropping packets.

c) The Contractor must verify these metrics with appropriate test equipment at EC's request.

d) Network Availability must be at least 99.9%.

i. Network Availability will be calculated by dividing the network available time by the total time in a calendar month, expressed as a percentage.

ii. Network unavailability caused by scheduled maintenance activity is excluded from the measurement of Network Availability

8.2. Service Portal

8.2.1. The Contractor must provide the following near real-time network statistics through the Service Portal:

a) traffic in bits per second

b) percent utilization

c) TX and RX errors and discards

d) total bytes transferred

e) average packet length

f) maximum bytes transferred per hour by day for send and receive per network segment

g) latency in millisecond

h) jitter in milliseconds

8.2.2. The Contractor's core network must have "self-healing" properties and attributes such that customer traffic is automatically rerouted to support sub-second recovery from fibre or equipment failures.

9. Service Requirements

9.1. Fibre Connectivity

The Contractor must connect their single mode fibre network through a media converter or other appropriate device to an Ethernet switch port in the EC's server room or LAN room in each building.

PART III – MANAGED WIDE AREA NETWORK

As and when requested by EC, the Contractor must provide managed MPLS based MAN/WAN infrastructure.

10. Use of Connecting Multiprotocol Label Switching Equipment

The Contractor must use the existing Connecting Equipment from the Access Area to the Service Delivery Point (SDP) when specified by EC. Figure 4 below illustrates how Connecting Equipment from a Contractor POP must be connected to an EC SDP.

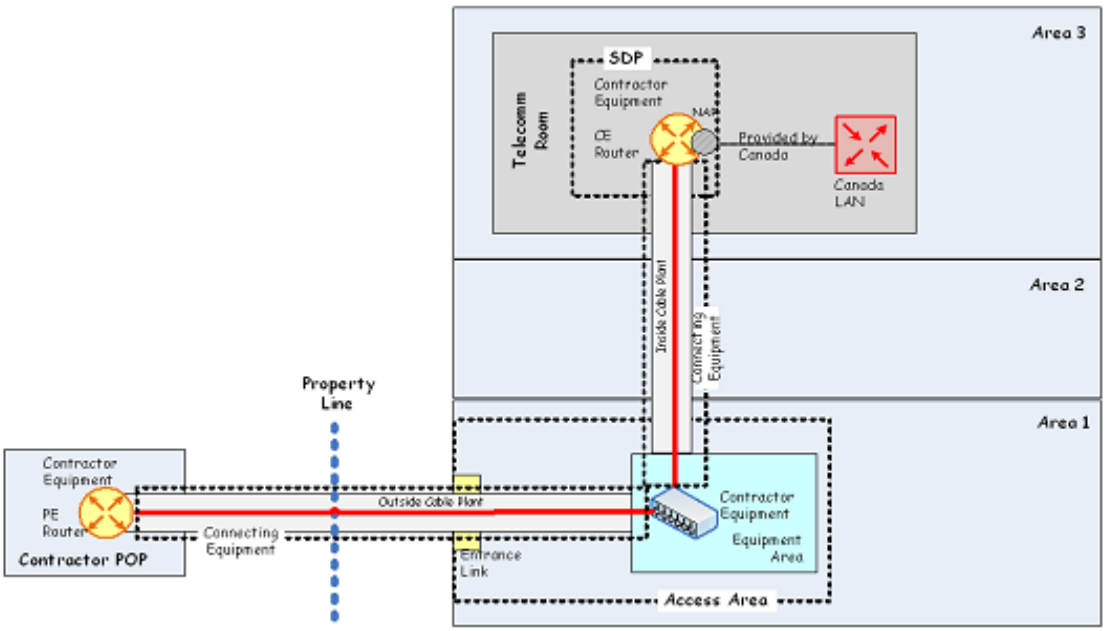

Figure 4: Connecting Equipment from Contractor POP to EC SDP

11. Internet Protocol Version 6

The MAN/WAN Services must route IPv6 packets using IPv6, 6VPE [IETF 4659] between SDPs and over the core network at no additional cost to EC. The Contractor must not use tunneling techniques from the CE Routers to provide IPv6 functionality.

12. Service Provisioning

12.1. Service Provisioning Process

Figure 5 illustrates the Service Provisioning Process, as further described below.

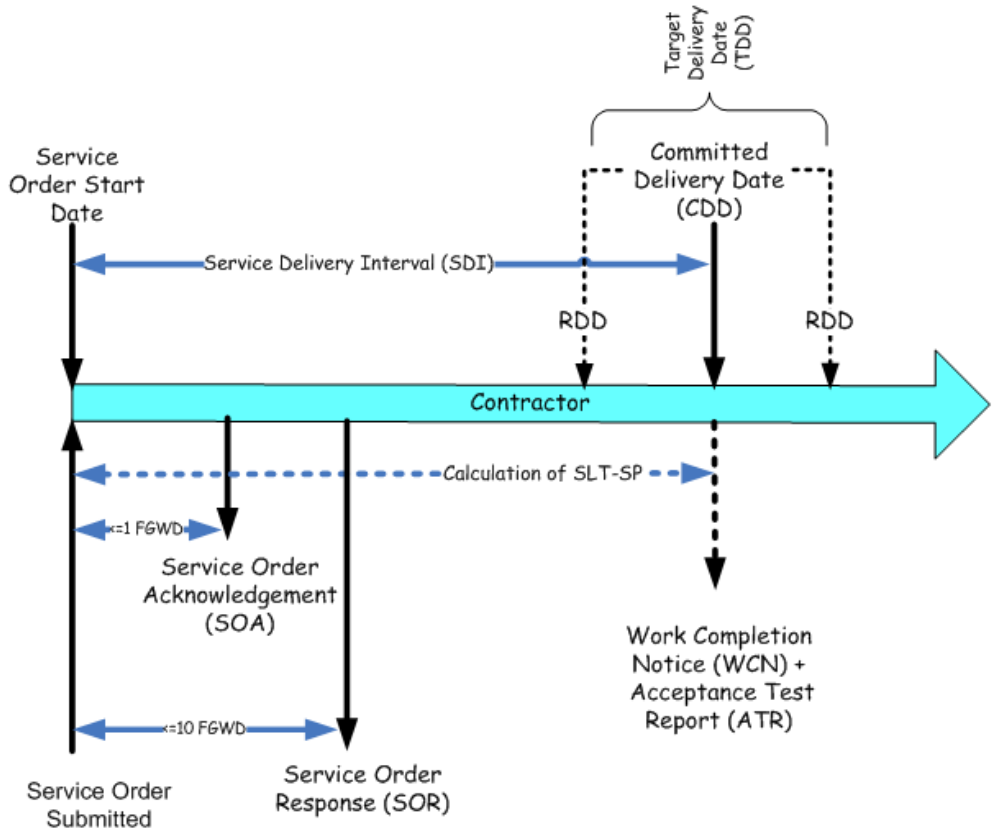

Figure 5: Service Provisioning Process

12.2. Service Orders

12.2.1. EC will issue a Service Order to the Contractor to perform, modify or reduce work that is to be provided under the Contract on an as-and-when requested basis.

12.2.2. Whenever the Contractor receives a Service Order from EC, the Contractor must

provide the Services ordered in accordance with the terms and conditions and at the prices and rates set out in the Contract. Regardless of when a Service Order is issued, all Service Orders automatically end no later than the last day of the Contract Period, and EC is not required to cancel any Service Orders at the end of the Contract Period.

12.2.3. The Contractor will not be paid for providing information required to prepare or issue a Service Order.

12.2.4. Service Orders can be issued by EC to order Services 24 hours per day, 7 days per week and 365 days per year.

12.2.5. The Contractor must begin work immediately for a Service Order when the Service Order is received from 9:00 a.m. to 5:00 p.m. (Eastern Time [ET]) on a Business Day, and at 9:00 a.m. (ET) the next Business Day if the Service Order is received between 5:00 p.m. and 9:00 a.m. (ET) or on a day that is not a Business Day. Notwithstanding the above, the Contractor must begin the work immediately for an Emergency Service Order, regardless of the time of day and/or day of the week that the Service Order is received.

12.2.6. The Contractor must perform the work for Service Orders in accordance with the Service Request fulfillment processes.

12.2.7. EC can designate a Service Order as an Emergency Service Order.

12.2.8. The Contractor must update the Service Order status in the Service Portal within one Business Day of receiving the Service Order.

12.2.9. The Contractor must provide a Service Order Acknowledgement within one Business Day of receiving a Service Order, and within one hour of receiving an Emergency Service Order.

12.2.10. The calculation of the Service Delivery Interval (SDI) for a Service Order for the purpose of calculating Service Credits starts on the date and at the time the Service Order is transmitted to the Contractor when the Service Order is received from 9:00 a.m. to 5:00 p.m. (ET) on a Business Day, and at 9:00 a.m. (ET) the next Business Day if the Service Order is received between 5:00 p.m. and 9:00 a.m. (ET) or on a day that is not a Business Day.

12.2.11. The Contractor must not reject a Service Order. If the Contractor requires clarification of a Service Order, the Contractor must request the clarifications within one Business Day for a Service Order, or within one hour for an Emergency Service Order. The Contractor must continue to meet the SDI for the Service Order regardless of the

clarification process and the time taken for clarifications.

12.2.12. EC will include the following information in each Service Order and, provided all this information is included, the Contractor must proceed with the fulfillment of the Service Order:

a) date Service Order transmitted to Contractor

b) Service Order identifier

c) Service Order type (normal, emergency)

d) Service Order Period (start and end date)

e) EC Contract identifier

f) details of any financial coding to be used

g) SDP Identifier (SDPID)

h) work location of an EC SDP, which can include:

i. civic address

ii. street address

iii. legal land description

iv. latitude and longitude

i) identification, quantity, and description, basis of payment of the Work being ordered by Service Catalogue Item with associated Service Catalogue Identifiers (SCIDs)

j) Committed Delivery Date (CDD), which is based on the SDI

k) Requested Delivery Date, which can be the CDD, a date before the CDD, or a date after the CDD

l) SDP contact name

m) SDP contact phone number

12.2.13. All Service Order interactions between EC and the Contractor (e.g. Service Order, Service Order Acknowledgement, Service Order Response, Work Completion Notice) must be conducted using one or more of the following:

a) e-mail with message headers and content specified by EC

b) e-mail with XML file attachments with markup and content specified by EC

c) XML file attachments with markup and content specified by EC transmitted electronically using a secure file transfer mechanism approved by EC

d) the Service Portal

12.3. Requested Delivery Date

12.3.1. The Contractor must deliver the work identified in a Service Order in accordance with the Service Level Target (SLT) for Service Provisioning as specified by the Service Delivery Interval, within the time period specified in the Service Order or, if not specified in the Service Order, in accordance with the terms of the Contract.

12.3.2. EC may request that the Contractor accept a Service Order with an RDD shorter than the CDD. If the Contractor agrees to the shorter RDD, EC agrees that the calculation of the SLT will be based on the standard SDI for the type of Service Order submitted (not the shorter SDI based on EC's RDD). If the Contractor agrees to the shorter RDD, the Contractor must make its best efforts to meet the shorter RDD.

12.3.3. The Contractor must accept a Service Order with an RDD that is longer than the CDD. The calculation of Service Credits will be based on the longer SDI as determined by the RDD.

12.3.4. The Contractor must provide a Service Order Response (SOR) within 10 Business Days of receiving a Service Order. The SOR must identify the Contractor's Target Delivery Date (TDD).

12.4. Issuing a Request for Unscheduled Work Estimate

12.4.1. EC will issue a Request for Unscheduled Work Estimate to the Contractor in the following circumstances:

a) Committed Traffic Rate (CTR) for a New SDP

b) the CTR requested by EC for an Existing SDP is not in the Service Catalogue

c) the SLT for service availability (SLT-SA) requested by EC for an Existing SDP is not in the Service Catalogue

d) the SLT for maximum time to restore service (SLT-MTRS) requested by EC for an Existing SDP is not in the Service Catalogue

e) Elections Canada requests a dual Access Link option that is not in the Service Catalogue

12.4.2. The Request for Unscheduled Work Estimate will be issued in order to obtain the Ceiling Monthly Price (CMP) for a CTR where EC will specify the:

a) CTR

b) SLT-SA

c) SLT-MTRS

d) implementation of a dual Access Link option

e) Ceiling Unit Price (CUP) for Connecting Equipment

12.5. Request for Unscheduled Work Estimate Response

12.5.1. The Contractor must provide a Request for Unscheduled Work Estimate Response to EC for a Request for Unscheduled Work Estimate within the Service Delivery Interval (SDI), which includes the time required for any visits to an SDP to obtain information for a Request for Unscheduled Work Estimate Response.

12.5.2. The Request for Unscheduled Work Estimate Response must be valid for a period of 30 Business Days (Request for Unscheduled Work Estimate Response Period) from the issuance of the Request for Unscheduled Work Estimate Response and represent the maximum cost for the Request for Unscheduled Work Estimate. Upon EC issuing a Service Order, the CMP and/or CUP will be included in the Service Catalogue in accordance with the Request for Unscheduled Work Estimate process for amending the Service Catalogue described further below. If EC does not issue a Service Order within the 30 Business Days, the Request for Unscheduled Work Estimate Response expires.

12.5.3. The Contractor will not be paid for providing a Request for Unscheduled Work Estimate Response.

12.5.4. When EC issues a Request for Unscheduled Work Estimate, the Contractor must include the following in its Request for Unscheduled Work Estimate Response:

a) a Ceiling Monthly Price (CMP)

b) a Ceiling Unit Price (CUP), where required, for a Facility Build of Outside Cable Plant from the Contractor POP to the Contractor Equipment in the Equipment Area

c) a CUP, where required, for a Facility Build of Inside Cable Plant

12.5.5. When requested by EC, the Contractor must provide the following supporting information for the Facility Build (as specified by EC) within 20 Business Days of a request:

a) detailed work breakdown structure that describes the milestones, schedule and resources to complete the Facility Build;

b) an assessment of existing Connecting Equipment to justify the implementation of new Connecting Equipment for a Facility Build including:

i. cable distance, including start and end points

ii. diagrams of existing and new Connecting Equipment

iii. justification for the number of copper pairs or fibre strands

c) a detailed cost breakdown for Facility Build activities and materials including:

i. Connecting Equipment material

ii. cable distance including start and end points

iii. trenching

iv. implementation of dual Access Links to an SDP

v. implementation of diverse entrances to a building

vi. X-rays

vii. core holes (number and size)

viii. conduit and duct banks (size, quantity, etc.)

ix. cable type and quantity (i.e., copper pairs, fibre strands)

x. use of forklifts, scissor jacks, etc.

xi. engineering labour hours, hourly rate and markup percentage

xii. installation labour hours, hourly rate and markup percentage

xiii. project management hours, hourly rate and markup percentage

xiv. security guard hours, hourly rate and markup percentage

xv. other costs (with explanation)

xvi. all costs from third parties involved in the work as evidenced by invoices from the third parties, together with additional information with the same format and content as described above for the detailed cost breakdown

12.5.6. Where the supporting information for a Facility Build indicates a lower cost for the work, the Contractor must:

a) provide an updated Request for Unscheduled Work Estimate Response that reflects the lower costs indicated in the supporting information; and

b) invoice EC in accordance with the lower cost in the updated Request for Unscheduled Work Estimate Response.

12.5.7. Where EC has requested supporting information, the Contractor must not invoice for EC MAN/WAN Services Facility Builds until EC has received the supporting information.

12.5.8. The Request for Unscheduled Work Estimate Response cannot include costs for work activities and materials for any other customer of the Contractor at the SDP.

12.5.9. EC is not required to issue a Service Order after receiving a Request for Unscheduled Work Estimate Response.

12.5.10. EC can issue one or more Service Orders after receiving a Request for Unscheduled Work Estimate Response.

12.5.11. EC may reject a Request for Unscheduled Work Estimate Response that does not include all the required information. EC's rejection of a Request for Unscheduled Work Estimate Response does not alter the Contractor's obligations for delivery of the Request for Unscheduled Work Estimate Response in accordance with the SLT for service provisioning (SLT-SP).

12.5.12. The Contractor must provide a Request for Unscheduled Work Estimate Response for up to three alternative solutions when requested by EC. EC, at its option, may also specify alternative solutions that the Contractor must analyze and include in the Request for Unscheduled Work Estimate Response. The Contractor must uniquely identify each proposed option (e.g. option A, option B) so that it could be specifically called up in a Service Order, provide a pros and cons analysis of each option that includes cost factors, and provide a recommendation of which solution should be implemented by EC, stating the reasons why. (Option A must always be presented as the Contractor's recommended solution.)

12.6. Cancelling, Suspending and Modifying Service Orders

Once a Service Order has been issued to the Contractor:

12.6.1. EC may cancel a Service Order at any time up to five Business Days before the Requested Delivery Date (RDD) at no cost to EC; provided, however, that if EC cancels the implementation of a Service after receiving the Service Order Response and the Contractor has irrevocably committed to the rental of facilities from a third party, or has incurred one-time costs, consideration will be given to reimbursement of those costs to the Contractor if that work was clearly described in its Request for Unscheduled Work Estimate Response. The Contractor must provide proof satisfactory to EC that the costs were actually incurred and the facilities were not, or will not be, re-used for another purpose.

12.6.2. EC may suspend and re-instate a Service Order within five Business Days before RDD at no cost to EC. However, if the Contractor has irrevocably committed to the rental of facilities from a third party, or has incurred one-time costs after the RDD, consideration will be given to reimbursement of costs to the Contractor incurred between the original RDD and the revised RDD. The Work must have been clearly described in its Request for Unscheduled Work Estimate Response. The Contractor must provide proof satisfactory to EC that the costs were actually incurred after the original RDD and the facilities were not, or will not be, re-used for another purpose.

12.6.3. When EC issues a Service Order to terminate a Service (i.e. places an out order), the Contractor must cease billing for that Service within one Business Day of the Requested Delivery Date in the Service Order for the cancellation.

12.7. Service Catalogue Updates

12.7.1. In light of the fact that technology and business models evolve quickly in the network services market, the Contractor acknowledges that EC's intention is to offer robust, comprehensive, and up-to-date wide area network services to its users throughout the Contract Period.

12.7.2. The Service Catalogue can be updated for:

a) new variants of existing Service Catalogue Items (e.g. NAPs, CTRs)

b) co-location of EC's telecommunications equipment at Contractor POPs

c) new Services (e.g. data compression, secure authentication and encryption of data traffic between NAPs)

12.7.3. The price of these updates will be negotiated on a case-by-case basis (as set out in the Article entitled "Basis of Payment" of the Articles of Agreement) and will be reflected through a Contract Amendment. Other than new variants of existing Service Catalogue Items, any change to the Service Catalogue will not be introduced to the Contract until at least six months after EC accepts the work performed during the Migration Readiness Stage.

PART IV – GENERAL REQUIREMENTS

The following sections are applicable to services in Part II – UNMANAGED Metropolitan Area Network and Part III – MANAGED Wide Area Network.

13. Change Management

13.1. Non-Event

Between Electoral Events the Contractor must provide a minimum notification of 30 Business Days for any changes to the network that could affect EC.

13.2. Event and Event Readiness

During Electoral Events and the period leading up to an Electoral Event (known as event readiness) only emergency changes that could affect the integrity of the network will be permitted. These include, but are not limited to, changes related to remediating hardware, network operating systems and network application vulnerabilities. Should emergency changes be required, EC must be notified in writing prior to implementation. If possible, emergency changes must be implemented during maintenance windows or between midnight and 6:00 a.m. (ET). EC will make the Contractor aware of periods of Electoral Events and event readiness.

14. Elections Canada's Responsibility for Content Transmitted over the Network

EC is solely responsible for any content that it, or that any person it permits to use the EC MAN/WAN Services being provided under the Contract, transmits or receives using those EC MAN/WAN Services.

15. Service Management

The Contractor must ensure the availability and operationalization of EC network services 24 hours a day/365 days a year for the duration of the Contract.

15.1. Contract Management Office

15.1.1. The purpose of the Contract Management Office is to ensure efficient and effective management of the contractual relationship developed in this Contract. The Contract Management Office must be the point of contact between EC and the Contractor for contract management.

15.1.2. Within five Business Days of Contract award, the Contractor must operationalize a Contract Management Office and maintain the Contract Management Office from 8:00 a.m. to 5:00 p.m. (ET) during Business Days for the duration of the Contract.

15.1.3. The Contractor must provide a telephone number and e-mail address for EC to contact the Contract Management Office.

15.2. Key Resources

The Contractor must provide two Key Resources (Service Operations Manager and Network Architect) to manage the business and technical aspects of the Contract.

15.2.1. Service Operations Manager

a) The Contractor must provide a Service Operations Manager (SPOC) that will manage the service level targets/agreements set forth in this Contract.

b) The Service Operations Manager must:

i. be EC's day-to-day point of contact for the Contract Management Office

ii. facilitate contract management review, operational, and service provisioning meetings

iii. liaise with the EC Contracting Authority and Technical Authority

iv. provide status updates/presentations to EC on incidents, problems, root cause analysis, etc.

v. facilitate any necessary contract amendment discussions

vi. ensure that any management and service level reports specified in the Contract are prepared and delivered to EC in a timely manner

vii. manage the prioritization, resolution and escalation of Contract issues, incidents, problems, and complaints

viii. create and maintain a log of Contract issues and action items

c) The Service Operations Manager must have a minimum of five years of experience

in the following:

i. serving as the single point of contact for managing the escalation of service management and service delivery issues, problems and complaints

ii. serving as a single point of contact and liaison for service desk issues and associated processes

iii. facilitating communications and integration with the client's service desk

iv. assessing service level compliance

v. assessing service performance

vi. reconciling service credits

vii. implementing best practices for service management, service delivery and service improvement

15.2.2. Network Architect

a) The Contractor must provide a Network Architect who will be EC's main point of contact for engineering, design and architecture services related to the Contract.

b) The Network Architect must facilitate network design and engineering meetings and any technical working groups to review and update any design issues.

c) The Network Architect must have a minimum of five years of experience in the following:

i. serving as the single point of contact and liaison for the planning, engineering, design and architecture of MAN/WAN Services

ii. documenting and analyzing network requirements, assessing the impacts to the client's MAN/WAN Services and recommending network changes, upgrades, and functional enhancements

iii. ensuring that Service Design and engineering reports are prepared and delivered to the client

iv. facilitating network design and engineering meetings and any technical working groups

v. reviewing and updating the Service Design

15.2.3. All Key Resources must be accessible from 8:00 a.m. to 5:00 p.m. (ET) during Business Days using office phone, cellular phone and e-mail.

16. Service Monitoring, Reporting and Documentation

16.1. Monthly Reports

16.1.1. The Contractor must provide monthly service reports detailing the following:

a) Network Availability

b) Incidents reported by EC

c) Incidents reported by the Contractor

d) average repair time by severity

e) outstanding Service Requests

16.1.2. Monthly service reports are primarily used by EC to monitor and assess the delivery of Work by the Contractor, provide EC with detailed information required for service assurance and are used in operational, service provisioning and contract management review meetings.

16.2. Report Delivery

16.2.1. The Contractor must ensure that all reports and documentation for MAN/WAN Services are accessible to EC through the Service Portal.

16.2.2. Each report must be delivered to the Technical Authority via e-mail within two business days following the end of each month.

16.2.3. Each report must report on the month that just ended and must provide year-to-date totals and averages per month of items listed in the monthly service report for the previous 12 months.

16.2.4. The Contractor must provide to EC all annual reports that are required under the Contract each year within 30 business days of the end of the previous 12 months based on the anniversary of the Contract.

16.2.5. The Contractor must provide to EC all weekly reports that are required under the Contract each week within two Business Days of the end of the previous week, where the end of each week is 11:59 p.m. (ET) Friday.

16.2.6. The Contractor must provide to EC all monthly reports that are required under the Contract each month within five Business Days of the end of the previous month where the end of each month is 11:59 p.m. (ET) on the last Business Day of the month.

16.3. Acceptance of Report Content and Format

16.3.1. The Contractor must define the content and format of reports and documentation, including how the reports are organized and hosted on the Service Portal, in consultation with EC and subject to EC's acceptance.

16.4. Report Language

16.4.1. The Contractor must provide reports and documentation in English using the above-accepted format.

16.5. Report Design

16.5.1. All reporting must be designed and maintained for efficient viewing and use online via the Service Portal and when downloaded to a User's desktop application (e.g. Microsoft Excel). As an example, reports that can be downloaded should have column widths that are sized appropriately for the field lengths. Downloaded reports should be formatted such that, whenever possible, they can be printed in an efficient manner. Downloaded reports must include headers and footers with report titles, file names, worksheet names, page numbering, etc.

16.5.2. The design of the reports must:

a) not require EC to reformat them in order to make them more usable or presentable

b) present information in a clear manner, including order of data, conditional formatting based on data content, and formatting of report headings, etc.

c) allow EC to generate reports using functions such as date range selection using calendars, sorting capability, partial field entry for searches and report building, and the ability to export reports to desktop applications like Microsoft Word, Microsoft Excel and Portable Document Format (PDF)

d) allow statistical and numerical reports to be downloaded in Microsoft Excel format; information representing numbers and dates must be downloadable as numbers and dates, and not formatted as text

16.5.3. All documentation, including reports, that is developed by the Contractor and provided to EC must meet the following minimum requirements:

a) The first page must be the title page and include:

i. document title

ii. authoring organization's name

iii. date of issue

iv. version number

b) The second page must contain the document history table and include:

i. date the document was revised ("Revision Date")

ii. name and the author who made the revision ("Modified By")

iii. version number of the document representing the revision ("Version")

iv. brief description of the changes made to the document ("Revision Description")

v. the third page must contain the table of contents

c) All subsequent pages must contain a header and/or footer with the following:

i. page number

ii. authoring organization name

iii. document title

iv. document tile name

v. revision number

vi. revision date

d) All documents must include the following sections:

i. introduction

ii. purpose

iii. intended audience

iv. references

16.6. Version Control

16.6.1. The Contractor must exercise strict version control for all reports. All reports must clearly display a version number and date and time of issue. All reports must clearly display the title and the period that the data in the report covers.

16.6.2. The Contractor must identify the most current version of reports as distinct from previous versions by, for example, locating them in separate lists, tables, tabs, etc.

16.6.3. The Contractor must notify EC representatives of any pending and completed revisions to documentation, based on a distribution list provided by EC.

16.6.4. The Contractor must ensure that all documentation is kept current and up-to-date at all times.

16.7. Changes to Reports

16.7.1. The Contractor must not make any structural changes (format, content provided) to an approved report without following the Service Request fulfillment process.

17. Service Operations

17.1. Service Desk

17.1.1. The Contractor must provide a Service Desk that performs the following functions:

a) acting as the primary point of contact for EC MAN/WAN Service Incidents 24 hours per day, 7 days per week and 365 days per year

b) answering and continuing the subsequent dialogue using the official language of Canada (French or English) requested by the EC authorized representative

c) interacting to record, track and resolve incidents with EC's representatives as designated by EC

d) providing a toll-free telephone number (e.g. 1-800 number) for EC authorized representatives to contact the Service Desk

e) providing a single e-mail address for EC authorized representatives to contact the Service Desk

17.1.2. The Contractor must provide a Service Desk with sufficient personnel with the

appropriate skills and experience who are knowledgeable about the EC MAN/WAN Services.

17.2. Operations Centre

17.2.1. The Contractor must provide a primary Operations Centre that is within Canada and has the infrastructure and resources required for the centralized management and operation of the EC MAN/WAN Services, 24 hours per day, 7 days per week and 365 days per year.

17.2.2. The Contractor must provide a backup Operations Centre within Canada, located at least 150 kilometers from the primary Operations Centre, that provides all operational and management functionality supported by the primary Operations Centre.

17.2.3. In the case of an outage at the primary Operations Centre, the transition to the backup Operations Centre must be seamless to EC and not affect the operations of the EC MAN/WAN Services.

17.2.4. The Contractor's resources supporting the primary and secondary Operations Centres must be located in separate buildings.

17.2.5. The Contractor must staff its Operations Centres with personnel with the skills and experience necessary to operate EC MAN/WAN Services.

17.3. Security Operations Centre

For its Security Operations Centre, the Contractor must meet the security requirements (SRs) referenced in SR-192, SR-316, SR-323, SR-545, SR-550, SR-552, SR-554, SR-557, SR-574, SR-575, SR-580, SR-582, SR-583, SR-584 and SR-585 of Appendix C – SOW Security Requirements.

17.4. Service Portal

17.4.1. The Contractor must meet the security obligations referenced in SR-90, SR-633, SR-658, SR-659 and SR-663 of Appendix C – SOW Security Requirements.

17.4.2. Within 60 Business Days of Contract Award, the Contractor must provide, and receive EC's acceptance of, a secure web portal (the Service Portal). The Service Portal must be accessible by using a web browser for a minimum of five concurrent Users 24 hours per day, 7 days per week and 365 days per year.

17.4.3. The Service Portal must provide an intuitive web-based user interface to deliver ease of use. This includes aspects such as presentation, organization, navigation, report generation and search tools.

17.4.4. The Service Portal must include the following features and functionalities:

a) a minimum of five Service Portal accounts

b) an English and a French interface that allows Users to select the English or the French interface upon logon to the Service Portal

c) orientation and introduction pages with Contractor contact information as specified by EC

d) an online context-sensitive help function

e) landing pages that enable EC to access information and navigate efficiently, including a landing page that, for example:

   i. includes separate sections for Incident, Problem and Service Request Tickets that are in an active state

   ii. summarize the active tickets by categories, as specified by EC, that allow EC to drill down to individual tickets by use of hyperlinks

   iii. provides a listing of any tickets currently in progress when a specific category is selected, allowing EC to hyperlink to the individual tickets and providing enough information for Users to be able to determine effectively which ticket they are searching for or wish to access

f) on-line self-registration of Users that includes:

   i. a form to enter User profile information including challenge/response questions

   ii. a checklist that presents the rules the password must comply with, and checks these rules positively as they are satisfied as the User chooses or changes their password

   iii. on-line registration request review and approval by Users designated by EC;

   iv. access profile selection

   v. automated e-mail registering the User with the Service Portal account username and password following approval of the registration

g) role-based access controls that define the rights (i.e. read/view, write/modify, delete, download) that a User has when accessing Service Portal pages,

applications and EC MAN/WAN services management data accessible on the Service Portal

h) an Access Profile for User accounts so that the User inherits the role-based access controls defined for the Access Profile

i) a "least privilege policy", as defined in Appendix C – SOW Security Requirements, for all Service Portal accounts

18. Escalation

Should situations arise where escalation is required for incidents and/or problems, the Contractor must follow the escalation steps based on the resolution stages that are detailed below:

Incident/Problem Resolution Stage	Title
1 – Prioritization and support	Manager, Data Centre and Network Operations
2 – Investigation and diagnosis	Director, Information Technology Infrastructure Operations
3 – Resolution	Chief Information Officer

Table 2: Escalation

19. Information Technology Service Management

The Contractor must provide IT service management for EC MAN/WAN Services in English as described in this subsection available 24 hours per day, 7 days per week and 365 days per year.

19.1. Service Request Fulfillment Process

19.1.1. For its Service Request fulfillment process, the Contractor must meet the security obligations referenced in SR-560, SR-612 and SR-613 of Appendix C – SOW Security Requirements.

19.1.2. The Contractor must create at least one Service Request Ticket and set the status to open for each Service Request submitted by EC within one Business Day of receiving the Service Request. A Service Request Ticket must include the following dedicated information fields for each Service Request:

a) Contractor Service Request Ticket number

b) Service Request description

c) date and time stamp when Service Request was initiated

d) date and time stamp when Service Request was closed

e) location of Service Request activity

f) Service Request category (normal, emergency, SDP Access)

g) reason for the Service Request

h) impact of the Service Request

i) risks associated with the Service Request

j) status of Service Request (i.e. open, closed, in progress, suspended, cancelled etc.)

k) affected SDP(s) and Transport Circuit(s)

l) Contractor contact (i.e. name, telephone number and e-mail address)

m) name of the individuals performing the Service Request

n) details on security clearance (i.e. security clearance level, expiry date, and date of birth and/or security clearance file number) of individuals (for SDP access)

o) EC contact information (i.e. name, telephone number and e-mail address)

p) activity log including all actions taken by the Contractor and third parties for the Service Request

q) related Service Order number (if applicable)

r) scheduled date and time for start/end of Service Request activity

s) actual date and time for start/end of Service Request activity

t) originator of the Service Request

u) planned outage time (if applicable)

v) actual outage time (if applicable)

w) Service Request approver's name

x) details of any support activities to be performed by the SDP contact(s);

y) the test activities to verify functional and operational integrity following the Service Request

z) back-out procedures to remove the changes and restore an EC MAN/WAN Service to its pre-Service Request state if the implementation of the Service Request fails

19.1.3. The Contractor must allow EC to submit Service Requests in English 24 hours per day, 7 days per week and 365 days per year:

a) to an e-mail address specified by the Contractor (with an automatic reply to confirm receipt of the e-mail)

b) electronically (with predefined forms and fields approved by EC) using the Service Portal

19.1.4. The Contractor must allow EC to approve Service Requests online using the Service Portal. To do this, in the Service Portal, EC must be able to fill in the following fields:

a) indicator of approval or rejection of the Service Request

b) name of EC approver

c) time and date of the approval

d) reason for non-approval

e) notes field

19.1.5. The Contractor must only accept approvals for Service Requests from authorized approvers specified in writing through the Service Portal by EC.

19.1.6. A Service Request may be submitted by the Contractor to change an EC MAN/WAN Service; however, the Service Request must follow the same fulfillment process.

19.1.7. A Service Request submitted by the Contractor with fewer than five Business Days notification must be categorized as an Emergency Service Request.

19.1.8. The Contractor must provide the following notices for a Service Request on the Service Portal as well as by e-mail when requested by EC:

a) Service Request Acknowledgement Notice within two hours of the receipt of the Service Request

b) Service Request Implementation Notice a minimum of 48 hours prior to the implementation of the Service Request

c) Service Request Cancellation Notice a minimum of 24 hours prior to the cancellation of the Service Request by the Contractor

d) Service Request Completion Notice within two Business Days of the completion of any Service Request

19.1.9. The Contractor must complete the Service Request activity – excluding Emergency Service Requests – in the maintenance windows approved by EC. This includes the planned primary outage time to complete the Service Request and secondary outage time required for back-out of the Service Request. Any service outage that extends beyond the maintenance window approved in the original Service Request will be treated as the service being unavailable and this period must be included in the calculation of SLT for Service availability (SLT-SA) and SLT for maximum time to restore service (SLT-MTRS). In such a case, the Contractor must initiate an Incident Ticket and record the time beyond the approved window as service outage time.

19.1.10. If the execution of a Service Request causes an unplanned impact or outage to EC MAN/WAN Services or it is determined that it will exceed the maintenance window approved by EC, the Contractor must contact EC immediately. EC may choose to ask the Contractor to suspend work immediately. If EC allows work to proceed, the Contractor must provide a complete explanation of the impact and the plan to restore service or complete the Service Request as quickly as possible. The Contractor must also initiate an Incident Ticket for any outage not identified in the Service Request.

19.1.11. The Contractor must automatically update a Service Request Ticket within 30 minutes of a change in work associated with the Service Request.

19.1.12. The Contractor must automatically provide Service Request Ticket information by e-mail to a distribution list where EC specifies the:

a) members of the distribution list

b) information from the Service Request Ticket

c) frequency of e-mail updates

d) distribution lists

e) criteria for selecting Service Requests (e.g., content of Service Request Ticket, Emergency Service Requests)

19.1.13. The Contractor must back out a Service Request, using the back-out procedures specified in the Service Request Ticket, when the Service Request has caused a disruption to EC MAN/WAN Services for more than two hours or when the Service Request did not achieve the objectives of the Service Request.

19.1.14. The Contractor must enter information in the Service Request Ticket log for a failed Service Request explaining the failure and change its status to unsuccessful within 30 minutes of completing the Service Request back-out procedures. The explanation must describe whether the back-out plan was used, what the current status is for the environment that was subject to the Service Request and what partial changes were implemented.

19.1.15. The Contractor must close the Service Request Ticket following completion of the Service Request activities.

19.1.16. The Contractor must provide a post-Service Request report that details actions taken to fulfill a Service Request to EC within five Business Days of a failed Service Request.

19.1.17. The Contactor must use a parallel cut process to implement Service Requests where existing equipment and facilities remain in place until the Service Request is successfully completed. A flash-cut/hot-cut process must only be used when pre-approved by EC.

19.1.18. The Contractor must disable or enable a NAP as specified by EC within one hour of a Service Request from EC.

19.1.19. The Contractor may not make changes during blackout periods of an Electoral Event without explicit written approval from EC.

19.2. Event and Incident Management

19.2.1. The Contractor must meet the security obligations referenced in SR-586, SR-591, SR-594, SR-597, SR-598, and SR-316 of Appendix C – Statement of Work Security Requirements.

19.2.2. The Contractor must proactively monitor EC MAN/WAN Services for Incidents 24 hours per day, 7 days per week and 365 days per year.

19.2.3. The Contractor must co-operatively work with EC and any other third parties as requested by EC to resolve Incidents.

19.2.4. The Contractor must maintain a list of critical SDPs and Transport Circuits, as specified by EC, which are to be treated with the highest priority. The Contractor must minimize

the mean time to restore service. EC may identify an SDP and a Transport Circuit to be critical that is not included in the list, or may request that reports on the status of the Incident resolution efforts be provided at a specific interval for any Incident it determines to be critical.

19.2.5. The Contractor must categorize and assign Incidents with a priority level in accordance with a scale specified by EC. Incident categorization and priority levels will be determined by EC within 40 Business Days after Contract Award.

19.2.6. The Contractor must create one Incident Ticket for each Incident immediately upon discovery of the Incident. For all Incidents, the Incident Ticket must include the dedicated information fields specified in SR- 599 of Appendix C – Statement of Work Security Requirements.

19.2.7. The Contractor must provide EC with a view of a single Incident Ticket for each Incident (i.e. not require EC to review multiple Incident Tickets for an Incident), accessible from the Service Portal.

19.2.8. The Contractor must allow EC to submit comments online within an Incident Ticket 24 hours per day, 7 days per week and 365 days per year using the Service Portal.

19.2.9. The Contractor must notify EC of Incidents, with priority levels specified by EC, within five minutes of detection of the Incidents. The notifications must be provided by e-mail to EC. If the Contractor does not receive acknowledgement of the notification from EC, the Contractor must inform the EC Manager of Data Centre and Network Operations by telephone.

19.2.10. The Contractor must provide EC with status updates of Incidents with priority levels specified by EC at a frequency specified by EC. The status updates must be provided by e-mail (and by telephone, when requested by EC if the Incident is severity one).

19.2.11. The Contractor must provide an estimated time for resolution with each update both verbally and within the Incident Ticket.

19.2.12. The Contractor must resolve Incidents by taking appropriate action to repair and restore EC MAN/WAN Services as quickly as possible in accordance with the SLT-SA and SLT-MTRS associated with the EC MAN/WAN Service.

19.2.13. The Contractor must ensure that all free-form text fields in Incident Tickets – such as progress/updates – root cause and resolution have clear descriptions using complete words, sentences and proper grammar.

19.2.14. The Contractor must document in the Incident Ticket activity log all:

a) management and technical escalations for Incidents

b) interactions with third parties

c) investigation, troubleshooting and analysis details, resolution activities and communications for Incidents in the Incident Ticket activity log

19.2.15. The Contractor must record in the Incident Ticket the date and time that each update is provided to EC and must record any direction EC provides related to the frequency of updates, change in priority and escalation, and include the name of the EC representative providing each direction.

19.2.16. The Contractor must track and report the outage time of each Incident in the associated Incident Ticket.

a) 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 EC – whichever occurs first.

b) The outage time for an Incident ends at the time that the EC MAN/WAN Service is fully restored for that Incident.

19.2.17. The Contractor must submit a request to the EC Manager of Data Centre and Network Operations for access to an EC SDP when access is required to resolve an Incident.

19.2.18. The Contractor must suspend outage time for an Incident at EC's request or where the Contractor has requested:

a) access to an SDP necessary to resolving an Incident, but EC is unable to provide access

b) closure of an Incident Ticket pending EC's approval, but EC is not available to consider the request

19.2.19. The Contractor must restart the outage time for an Incident at the point where the outage time has been suspended when:

a) SDP access was required by the Contractor and EC grants access to the SDP

b) EC is available to review the request to close an Incident and has determined that the Incident must remain open

19.2.20. The Contractor must not alter the outage time for an Incident Ticket once the Incident

Ticket has been closed. Any required changes to outage time are facilitated through the adjusted outage time field within the Incident Ticket.

19.2.21. Where outage time for an Incident was suspended and the Contractor was able to resolve the Incident without access to the SDP (truck roll), the Contractor must include the suspended outage time in the total outage time for the Incident.

19.2.22. The Contractor must review the outage time recorded for an Incident Ticket with EC to ensure completeness of information and accuracy, and obtain EC's acceptance of the outage time.

19.2.23. The Contractor must update any and all affected reports within one Business Day of any change to outage times recorded in the Incident Tickets. The outage time must be reported as having occurred on the date of the actual outage regardless of when the associated Incident Ticket is opened or closed.

19.2.24. The Contractor must make a reasonable effort to investigate and resolve the Incident without requesting access to the SDP (i.e. remote diagnostics and consulting with third parties involved with the service delivery).

19.2.25. If an Incident Ticket is closed and a subsequent Incident occurs within 24 hours for the same Incident, the Contractor must re-open the original Incident Ticket or open a new Incident Ticket with a cross reference to the previous Incident Ticket, and calculate the outage time for the new Incident using the combined outage time of both Incidents, and record this time in the adjusted outage time field of the Incident Ticket.

19.2.26. The Contractor must review an Incident Ticket for completeness and accuracy within one Business Day of closing the Incident Ticket. The Contractor's review may result in the need for adjustment to the outage time recorded in the Incident Ticket. These adjustments must be referred to as adjusted outage time. When an Incident Ticket requires adjustment, the Contractor must enter the adjusted outage time in the corresponding field within the Incident Ticket. The adjusted outage time may be entered as either a positive or negative value depending on whether there is a need to add or subtract outage time. The Contractor must enter a comment to support the reason for any adjusted outage time.

19.2.27. The calculation of outage time for which the Contractor is accountable and that is to be included in the calculation of the service levels for SLT-SA and SLT-MTRS is outage time plus adjusted outage time.

19.2.28. The Contractor must work with EC to develop the outage time reconciliation process

within sixty days of Contract Award. The purpose of the process is to facilitate a joint review of Incidents and the measurement of outage times such that EC and the Contractor come to agreement on their values. The process must be designed to ensure that reconciliation of every Incident Ticket with outage time is completed expediently within three Business Days of the closing of an Incident Ticket. The process must include EC's online approval and acceptance of the outage times recorded in the Contractor's Incident Tickets.

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

19.2.30. The Contractor must develop workarounds to address Incidents with unidentified root causes.

19.2.31. The Contractor must provide a briefing that details any analysis and actions taken for an Incident within one Business Day of a request by EC for an Incident.

19.2.32. The Contractor must provide a Post-Incident Report detailing root cause analysis and the actions taken by the Contractor to resolve the incident within two Business Days of a request by EC. If EC finds the Post-Incident Report to be incomplete or inaccurate, it will advise the Contractor of the deficiency. Following such notification, the Contractor must re-issue the report addressing the deficiency within two Business Days. After one review, should EC continue to find the Post-Incident Report to be deficient, it will be considered as not delivered and EC will advise the Contractor of the start of Service Credits related to non-delivery of the report.

19.2.33. The Contractor must provide EC with ongoing updates for the action plans contained within its post-Incident reports. The Contractor must notify EC in advance when it becomes aware that it will not meet target dates specified in its action plans.

20. Security

20.1. Build Standards

20.1.1. The telecommunication infrastructures for all buildings must meet the requirements of Electronic Industries Alliance (EIA)/Telecommunications Industry Association (TIA) standards (568A-568B and 569), *Commercial Building Standard for Telecommunication Pathways and Spaces and cabling* (and addenda), and other relevant nationally recognized codes standards that ensure the integrity and security of cable pathways within the buildings.

20.2. Assessment of Products

20.2.1. The products that form part of EC MAN/WAN Services must be evaluated by a recognized certification body approved by EC, or evaluated by the Contractor by conducting a vulnerability assessment and functionality assessment to validate that the product (including both hardware and software) conforms to its stated security functionality, at no cost to EC. For Contractor assessments, test plans and test results must be provided to EC within 10 Business Days of a request by EC. EC reserves the right to independently validate and approve the products. EC-approved and recognized certification bodies include but are not limited to:

a) Common Criteria (CCS): http://www.commoncriteriaportal.org/

b) Cryptographic Module Validation Program (CMVP): http://csrc.nist.gov/groups/STM/cmvp/validation.html#02

20.2.2. When any Contractor provided equipment is returned, the configuration and user data must be purged immediately in accordance with the Canadian Security Establishment (CSE) ITSG-06 and security considerations for the use of removable media devices for Protected C and classified information must be also purged immediately as well in accordance with the CSE ITSB-112 directive.

20.3. Network Management Protocols

20.3.1. The Contractor must ensure that hardware and software used to deliver EC MAN/WAN Services can be managed using security protocols that use EC-approved cryptographic algorithms and key sizes.

20.3.2. The Contractor must not use port forwarding or IPSec for transport of protocols with known vulnerabilities and/or considered insecure by EC, including Telnet, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) and Hypertext Transfer Protocol (HTTP), unless approved by EC.

20.4. Security Monitoring and Incident Reporting

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

20.4.2. The Contractor must immediately report to EC any Incidents relating to the security of EC MAN/WAN Services or EC Data including but not limited to those Incidents listed in the preceding paragraph. For example, any Unauthorized Access or attempt to gain

Unauthorized Access must immediately be reported. Also, the discovery of any virus or malicious code and/or the installation of any unauthorized software code on any equipment must immediately be reported.

20.4.3. The Contractor must cooperate fully with EC in the investigation of any Security Incident. The Contractor must meet the security obligations referenced in SR-113, SR-239, SR-546, SR-547, SR-548, SR-580, SR-581, SR-586, SR-590, SR-594, SR- 595, SR-600, SR-601, SR-602, SR-603, SR-605, SR-606 and SR-612 of Appendix C – Statement of Work Security Requirements.

20.4.4. During a Security Incident, the Contractor must reduce the standard response time according to the priority of the Security Incident as articulated by the Contractor as part of the response to the Security Requirements in Appendix C. EC will specify the reduced response time based on the response time articulated by the Contractor.

20.4.5. The Contractor must provide a high-level assessment of the protection level that would be provided by EC MAN/WAN Services based on an attack/threat scenario provided by EC (e.g. is EC protected against this attack/threat?) within eight hours of a request by EC. A detailed assessment of the protection level must follow within two Business Days of the request by EC.

20.4.6. The high-level assessment must provide EC with an indication of the existence of a potential impact and the anticipated extent of that impact to the EC MAN/WAN Services. The detailed assessment must identify the specific network components that may be or are vulnerable to the attack/threat scenario.

20.4.7. The Contractor must assign a priority level for a Security Incident as set out in Table 3.

Service	Priority 1	Priority 2	Priority 3	Priority 4
Malware	EC MAN/WAN Services Infrastructure components infected One or more clients within the National Security Portfolio are impacted	Potential communication with botnet C&C or potential exfiltration of data Moderate likelihood of media interest	No external botnet communication established Low likelihood of media interest	Minimal to no business impact No media interest

	Communication established with botnet command and control (C&C) or exfiltration of data High likelihood of media interest			
Social Engineering	Communication established with botnet C&C High likelihood of media interest Breach of Protected C or Classified (Secret or Top Secret) information Privacy breach affecting EC	Potential for communication with botnet C&C Moderate likelihood of media interest Breach of Protected B or Classified (Confidential) information	No data exfiltration Breach of Protected A information	Spam
Denial of service	> 1 EC MAN/ WAN Services components are unavailable Major impact or highly visible to client business operations Affects a critical client service High likelihood of media interest	> 1 EC MAN/WAN Services component is unavailable or > 1 EC MAN/WAN Services components are affected and operationally degraded High impact or highly visible to client business	Limited impact or no negative effect on client operations Low likelihood of media interest	

		operations Moderate likelihood of media interest		
Unauthorized Access	EC MAN/WAN Services Data or client data EC MAN/WAN Services core Infrastructure EC MAN/WAN Services network Communication established with botnet C&C or exfiltration of data High likelihood of media interest	EC MAN/WAN Services access Infrastructure Service Portal Potential communication with botnet C&C or potential exfiltration of data Moderate likelihood of media interest	Contractor Management Restricted Zone Single User- level account No external communication established Low likelihood of media interest	Accidental leak of non- Protected or non-Classified information
Information Breach	Protected C or Classified (Secret or Top Secret) information Client data, EC MAN/WAN Services security data EC MAN/WAN Services network device configuration data	Protected B or Classified (Confidential) information EC MAN/WAN Services system data EC MAN/WAN Services management data	Protected A information	Leak of non-Protected or non-Classified information

Table 3: Priority Level Assignment for Security Incidents

21. Problem Management

21.1. Problem Management Requirements

21.1.1. The Contractor must proactively identify, investigate, diagnose, analyze (trend) and correlate Incidents in order to determine Problems and Known Errors.

21.1.2. The Contractor must designate three or more Incidents with the same root cause within a rolling 90-day window as a Problem.

21.1.3. The Contractor must designate network performance exceptions, where performance degradation has been identified by EC, as a Problem.

21.1.4. The Contractor must create a Problem Ticket for each Problem. A Problem Ticket must include the following dedicated information fields for all Problems:

a) Problem Ticket number

b) Problem description/details

c) date/time Problem Ticket logged

d) Problem status

e) Problem urgency

f) Problem impact

g) Problem priority

h) related Incidents Tickets

i) User details

j) Service details

k) equipment details

l) details of all diagnostic or attempted recovery actions taken

m) Problem trend analysis

n) resolution description and root cause

21.1.5. The Contractor must obtain EC's approval to close a Problem Ticket.

21.1.6. The Contractor must not suspend a Problem Ticket without EC's approval.

21.1.7. EC will specify the impact, urgency and priority of a Problem and the Contractor must assign the appropriately specified impact, urgency and priority to the Problem Ticket.

21.1.8. The Contractor must associate Incidents to existing or new Problems as requested by EC.

21.1.9. The Contractor must manage Problems through to resolution, ensuring that root cause is determined, preventive measures are implemented, and necessary "clean-up" is completed to remedy the Problem.

21.1.10. The Contractor must provide resolutions and targeted preventative actions for Problems and Known Errors including, for example: training, recommending procedural or process changes, and creating support documentation.

21.1.11. The Contractor must identify and investigate Known Errors until they are eliminated by the successful implementation of one or more Service Request(s).

22. Service Design and Engineering

22.1. Service Design and Engineering Requirements

22.1.1. The Contractor must initiate a Service Request for modifications, additions and deletions to the Service Design requested by EC. The Service Request Ticket must include a description of any Service Design options reviewed and any record of decisions.

22.1.2. The Contractor must provide engineering and design for EC MAN/WAN Services including:

a) integration with non-EC MAN/WAN Services and systems specified by EC

b) evaluating EC's technical, functional, and operational requirements

c) adapting, tuning, and improving EC MAN/WAN Services to ensure optimal performance

d) proactively assessing the capacity for EC MAN/WAN Services and providing

recommendations for capacity changes

23. Facility Management/Access to Crown Property

23.1. Service Delivery Point Access

23.1.1. The Contractor must communicate directly with SDP representatives identified by EC to arrange access to an SDP. The Contractor must open a Service Request and categorize it as an SDP access. The Service Request must include the following information:

a) date and time of the visit

b) name of all Contractor or subcontractor/third-party personnel who will participate in the visit

c) details on the security clearance level of each person visiting

d) expected duration of the visit

e) purpose of the visit, including the nature of the work to be performed during the visit (details on all buildings and rooms that are to be visited must be provided)

f) details of any type of support that the SDP contact is requested to provide during the visit

23.1.2. The Contractor must submit the Service Request for SDP Access a minimum of five business days prior to the date of visiting the SDP. Where an onsite visit to an SDP is required for emergency purposes, including Incident investigation and resolution or security issues, the SDP access will be coordinated through EC's service desk.

23.1.3. The Contractor must provide EC with a minimum of 24 hours' advance notice to change or cancel an approved Service Request.

23.1.4. The Contractor must not send any personnel to an SDP who have not been pre-authorized through a Service Request.

23.1.5. Where EC has previously approved access to an SDP as documented in a Service Request, and access was not provided by EC in accordance with the Service Request, the Contractor must again request access to the SDP within two business days of the denied access to the SDP. If the Contractor makes this request within two business days of the denied access to the SDP, the SDI for any associated SLT for service provisioning (SLT-SP) will be increased to include the time between the date that the

request for access to the SDP was resubmitted and the time of the rescheduled SDP access.

23.1.6. The Contractor must record in the Service Request any instance where it has exhausted all means of communication with EC's representatives at an SDP and where EC's representatives designated for access to an SDP were not available by including the following information:

a) the SDP location

b) the Client that controls access at that site

c) primary contact information for EC's representative at the SDP

d) the date and time that the Contractor attempted to make contact via all telephone numbers and e-mail addresses provided (with copies of any e-mails)

e) secondary contact information for EC's representative at the SDP

f) the representative to whom the request was made

23.1.7. If EC determines that coordination of the Contractor's visits to EC SDPs requires additional communication between the Contractor and EC's representatives, the Contractor must facilitate regularly scheduled calls between the representatives as frequently as every business day. EC will determine the required frequency of the calls. If necessary, the Contractor must make a telecom bridge available to connect multiple parties to the calls.

23.2. Restoration of the Equipment Area

23.2.1. The Contractor's Equipment will at all times remain the property of the Contractor. The Contractor, at the expiration or earlier termination of the right to use the SDP, at its cost must:

a) remove the Contractor's Equipment, all trade fixtures and all of the Contractor's personal property from the SDP

b) restore the SDP to EC's or the Crown's most current property standard (including, without limitation, the removal and disposal of any and all hazardous or toxic substances and their containers in accordance with all applicable laws and the requirements of all authorities and all required repairs and restoration of the roof of the property) to the extent required by EC

c) otherwise peaceably surrender and deliver up vacant possession of the SDP to EC (in as good order, condition and repair as the Contractor is required under these provisions to maintain and keep the SDP)

d) repair any damage caused to the property or any part of it by this removal or restoration

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

24. Acceptance Procedures for Contractor Work

24.1.1. The Contractor must submit all deliverables such as documents, plans, designs, etc. to EC for its review and acceptance. Upon receipt of any deliverable or portion of the Contractor's Work requiring EC's review and acceptance, EC will provide a written response to the Contractor within five Business Days.

24.1.2. All the Work is subject to inspection and acceptance by EC. Inspection and acceptance of the Work by EC do not relieve the Contractor of its responsibility for defects or other failures to meet the requirements of the Contract. EC will have the right to reject any Work that is not in accordance with the requirements of the Contract and require its correction or replacement at the Contractor's expense. EC's written response will either provide acceptance of the Work or will describe any deficiencies that the Contractor must correct in order to obtain EC's acceptance.

24.1.3. The Contractor must provide representatives of EC access to all locations where any part of the Work is being performed at any time during working hours. Representatives of EC may make examinations and such tests of the Work as they may think fit. The Contractor must provide all assistance and facilities, test pieces, samples and

documentation that the representatives of EC may reasonably require for the carrying out of the inspection.

24.1.4. The Contractor must inspect and approve any part of the Work before submitting it for acceptance or delivering it to EC. The Contractor must keep accurate and complete inspection records that must be made available to EC on request. Representatives of EC may make copies and take extracts of the records during the performance of the Contract and for up to three years after the end of the Contract.

24.1.5. EC may request meetings with the Contractor during its review period, and the Contractor may request meetings with EC following receipt of EC's notice of any deficiencies. EC will meet with the Contractor within two Business Days of the Contractor's request.

24.1.6. The Contractor must include time for this review and acceptance process within the Work delivery timeframe requirements specified in the Contract. For example, if the Contractor is required to provide the Service Design within 30 Business Days of Contract award, the Contractor must factor within that schedule EC's review of that deliverable and any subsequent meetings that might be required if there are deficiencies.

24.1.7. EC is not required to provide additional time to the Contractor if EC determines that the Contractor's Work is deficient and EC does not provide its acceptance. However, if EC does not provide a written response within five Business Days or EC is unable to meet with the Contractor within two Business Days of a request to review a deliverable, the Contractor's required delivery time frame specified in the Contract will automatically be extended by the same number of business days that EC delayed its response beyond the five Business Days, or delayed meeting with the Contractor beyond two Business Days.

24.2. Acceptance Form

24.2.1. The Contractor must develop an acceptance form to be used to obtain written acceptance from EC for the Contractor’s deliverables, completion of major project milestones, and any other Work requiring acceptance. The acceptance form must at a minimum include the following:

a) description of the project deliverable or milestone

b) required completion date for the deliverable or milestone (according to the Contract)

c) date the deliverable is submitted to EC for review and acceptance

d) fields for the name, date and signature of the Contractor's service manager who has reviewed and endorses the quality and completeness of the Work being submitted for acceptance

e) checkboxes for EC to indicate acceptance or rejection of the Work being submitted for acceptance

f) field for EC to enter the reason for rejecting the Work being submitted for acceptance

g) fields for the name, date and signature of the EC's Technical Authority

h) date that EC responds with acceptance or rejection of the Work being submitted for acceptance

i) date that EC meets with the Contractor (at the Contractor's request) to review the Work being submitted for acceptance

j) the number of Business Days that the delivery timeframe for the Work being submitted for acceptance is extended due to EC's delay (beyond five Business Days) in its review, or delay (beyond two Business Days) in meeting with the Contractor to discuss concerns about a deliverable

25. Service Level Targets

25.1. Service Level Target Overview

25.1.1. The Contractor must design, implement, manage and operate the EC MAN/WAN Services such that they meet the SLTs defined in this section.

25.1.2. The Contractor must count omitted SLT performance measurements as failed measurements, with the exception of performance measurements for the affected EC MAN/WAN Service that are in a failed state (i.e. an outage).

25.1.3. For all rounding of SLT measurements, the Contractor must use the symmetric arithmetic rounding up that rounds half-way numbers up. In this case, a "halfway" value such as 5.5 will round up to 6. Where three decimal places are required, a value such as 99.9445 will round up to 99.945, while the number 99.9342 will round down to 99.934.

25.1.4. All calculations of availability expressed as a percentage must be based on a minimum

of four decimal points rounded to the nearest three decimal points (e.g. 99.9784% would be equal to 99.978%).

25.1.5. The Contractor must monitor, measure, calculate, and report on service levels 24 hours per day, 7 days per week and 365 days per year, unless otherwise indicated for a specific SLT.

25.1.6. All service levels that the Contractor is required to measure and any associated test results must be accessible to EC via the Service Portal.

25.1.7. Outage time for an EC MAN/WAN Service begins from the time that the Incident is detected by the Contractor, or reported to the Contractor by EC – whichever occurs first. The outage time used in the calculations ends when the EC MAN/WAN Service is fully restored for the Incident.

25.1.8. A lack of proper security clearance by the Contractor, Contractor's resources or other individual identified to perform the Work does not preclude the Contractor from its obligation to restore the affected service within the SLT. Persons without current and valid clearances must not be allowed to perform the Work.

25.1.9. In cases where EC attempts to report an Incident for an outage where the Contractor's service desk does not answer the call, the start time for the outage begins at the time EC places the unanswered call to the service desk or when the Contractor detects the Incident – whichever occurs first. EC will timestamp and document the point at which a call was placed by EC.

25.1.10. The outage time used in the calculation of SLTs excludes any time whereby EC agreed to suspend the associated Incident Ticket and resumes when EC requests that the Incident Ticket be unsuspended.

25.1.11. The outage time used in the calculation of SLTs excludes the time for Service Requests approved by EC.

25.1.12. The failure of a NAP, for which outage time is calculated, includes any failure of the associated component of a Transport Circuit.

25.1.13. Any amendment to Service Level Targets for Service Availability (SLT-SA) must be agreed to in writing by both the Contractor and EC. Changes may require a Contract amendment if SLT-SA changes service catalogue pricing or service credit provisions.

25.2. Service Level Target for Service Availability

25.2.1. The SLT-SA is that service availability must be greater than or equal to 99.900%.

25.2.2. The period of measure for SLT-SA is monthly; therefore the total number of minutes in the measurement period will vary based on the number of calendar days in the month.

25.2.3. The Contractor must calculate SLT-SA as follows:

$$\frac{measurement\ period - sum\ of\ the\ outage\ times}{measurement\ period} \times 100$$

Example:

Measurement period (June): 30 days = 30 x 24 hours x 60 minutes = 43,200 minutes

Sum of all outage minutes for the NAP in the month: 98 minutes (excludes time associated with SLT- MTRS exception)

Calculation: ((43,200 - 98) / 43,200) x 100 = 99.773%

25.2.4. The outage time from the following events may be excluded from the calculation of SLT-SA as determined by EC during review of Incidents:

a) a failure occurs to equipment or facilities owned and managed by the Contractor, but due to redundancy and/or diversity implemented within EC MAN/WAN Service Infrastructure, the EC MAN/WAN Service is restored within a reroute timeframe of less than 100 milliseconds

b) a failure occurs related to a Security Incident where EC has approved mitigation actions that impact the service's availability

c) an outage occurs due to the loss of power at the SDP beyond the time period for power backup provided by the Contractor

d) the outage is associated with an approved Emergency Service Request that does not exceed a two-hour period and for which the Contractor has provided a post-Service Request report

e) the outage for a NAP with SLT-SA is determined to be due to the fibre cable being cut or damaged by a third party (i.e. a third party not performing Work for the Contractor)

25.3. Service Level Target for Maximum Time to Restore Service

25.3.1. The SLT-MTRS for a NAP is that the maximum time to restore Services must not exceed:

a) 2.0 hours during event periods when EC is engaged in delivering an Electoral Event)

b) 4.0 hours during non-Electoral Event periods

25.3.2. The measurement for SLT-MTRS is on a per-Incident basis.

25.3.3. SLT-MTRS is applicable for failures where the NAP has a SLT-SA, when the cause of the outage is due to the fibre cable being cut or damaged by a third party (i.e. a third party not performing Work for the Contractor).

25.4. Service Level Target for Service Desk Response

25.4.1. The SLT for service desk response (SLT-SDR) is that the Contractor's service desk must answer 90.000% of all telephone calls placed by EC within 20 seconds.

25.4.2. The period of measure for SLT-SDR is monthly.

25.4.3. The SLT-SDR must be calculated as follows:

$$\frac{\#\ of\ calls\ answered\ within\ 20.0\ seconds + \#\ of\ calls\ abandoned\ within\ 20.0\ seconds}{total\ \#\ of\ calls\ answers + total\ \#\ of\ abandoned\ calls} \times 100$$

25.4.4. The calculation of time to answer a call by the service desk begins when a caller starts waiting in queue for a Contractor's service desk agent and ends when the Contractor's service desk agent, a live person, answers the caller. Using voice scripts and menu options acceptable to EC, the calculation of time to answer a call excludes any time spent by callers listening and making menu selections in the Contractor's Interactive voice response system prior to waiting in queue for a Contractor's service desk agent.

25.4.5. An abandoned call to the service desk is a call that is connected to the Contractor's telephone system and the calling party terminates the call before a service desk agent answers the call.

25.5. Service Level Target for Service Portal Maximum Time to Restore

25.5.1. The SLT for Service Portal maximum time to restore (SLT-SPMTR) is that the Service Portal maximum time to restore is less than or equal to:

a) 4.0 hours from the start of any Incident where the a User is unable to access Incident Tickets, Service Orders or ad hoc and on-demand reports;

b) 8.0 hours from the start of any Incident where the User is unable to access any Service Portal function excluding access to Incident Tickets, Service Orders or ad hoc and on-demand reports.

25.5.2. The outage time used in the calculation of SLT-SPMTR begins from the time that the

Incident for the Service Portal is detected by the Contractor or is reported to the Contractor by EC – whichever occurs first. The outage time used in the calculation ends when EC's access to the Contractor's Service Portal functions is fully restored, as and when confirmed by EC.

25.5.3. In the event that Incidents occur for multiple functions on the Service Portal such that the outage times overlap, the outage time will be considered as continuous until all of the affected Service Portal functions are fully restored.

25.6. Service Level Target for Service Provisioning

25.6.1. The SLT-SP is that the service provisioning period must be less than or equal to the SDI as defined in Table 4.

25.6.2. The Contractor must calculate the time to complete the Work as the number of Business Days from the date of issuance of the Service Order or Request for Unscheduled Work Estimate to the Contractor, to the date that EC accepts the Work.

25.6.3. The SLT-SP is measured on a per-Service Order or per-Request for Unscheduled Work Estimate basis.

	SERVICE PROVISIONING DESCRIPTION	**SDI**
1	Implement a Transport Circuit where Facility Builds are not required.	30 Business Days
2	Provide a Transport Circuit where Facility Builds are required.	65 Business Days
3	Provide a Request for Unscheduled Work Estimate Response for a Transport Circuit including a detailed description and applicable SLT-SA and SLT-MTRS	20 Business Days

Table 4: Service Level Targets for Service Provisioning

25.7. Service Level Target for Service Delivery Response

25.7.1. The SLT for service delivery response (SLT-SDRES) is that the service delivery response time must be less than or equal to the SDI as defined in Table 5.

25.7.2. The Service Delivery Response time is the time for the Contractor to complete the Work associated with a Service Delivery Response. The Contractor must calculate the time to complete the Work from the time of issuance of the Service Request by EC for the Work until EC accepts the Work. For items where there is no explicit Service Request, the Contractor must deliver the deliverable in accordance with the section in

which the service is defined.

25.7.3. The SLT-SDRES is measured on a per-instance basis of the Work as specified by EC with a Service Request or as defined as a deliverable in the Contract.

	SERVICE DELIVERY RESPONSE DESCRIPTION	SDI
1	Service Portal administration: changes to access profiles, User accounts, role-based access controls	2 Business Days
2	Reset a User account password on the Service Portal	4 hours
3	Disable/enable a NAP	1 hour
4	Posting of weekly/monthly reports on Service Portal	5 Business Days
5	Delivery of post-Incident reports	2 Business Days
6	Delivery of Security Incident post-mortem report (SR-606)	72 hours
7	Notification security Operations Centre not available (SR-388)	15 minutes
8	Provide security Operations Centre acknowledgement of received e-mail (SR-584)	15 minutes
8	Invoice and associated Billing Detail Files	5 Business Days
9	Initiation of Service Request (per EC's request)	1 Business Day
10	Update to documentation and data repositories	10 Business Days
11	Update to Service Design document	20 Business Days
12	High level Security Incident assessment	8 hours
13	Detailed level Security Incident assessment	2 Business Days

Table 5 :Service Level Targets for Service Delivery Response

25.8. Service Level Target for Contractor Responsibilities

25.8.1. The SLT for Contractor responsibilities (SLT-CONRES) is that the Contractor responsibility must be completed in a time period less than or equal to the SDI as defined in Table 6.

25.8.2. The SLT-CONRES is measured as the time for the Contractor to complete the Work associated with a Contractor responsibility or Work. For items where there is no explicit EC request, the Contractor must deliver the deliverable in accordance with the section in which the service is defined.

25.8.3. The measurement for SLT-CONRES is on a per instance basis of the Work as defined in the Contract.

	CONTRACTOR RESPONSIBILITY DESCRIPTION	SDI
1	Update migration activity report for each SDP migrated	24 hours
2	Request clarifications for Service Orders (normal)	1 Business Day
3	Request clarifications for Emergency Service Orders	1 hour
4	Service Order Acknowledgement (normal Service Orders)	1 Business Day
5	Service Order Acknowledgement for Emergency Service Orders	1 hour
6	Service Order Response	10 Business Days
7	Creation of Service Request Ticket	1 Business Day
8	Service Request Cancellation Notice following cancellation	24 hours
9	Service Request Completion Notice following completion	2 Business Days
10	Update Service Request Ticket following a change in work	30 minutes
11	Notify EC of an Incident, based on priority levels specified by EC.	5 minutes
12	Outage time updates to affected service management reports	1 Business Day
13	Review and adjustment to outage times following Incident Ticket closure	1 Business Day
14	Briefing for an Incident following request by EC	1 Business Day
15	Mitigate high-risk vulnerability (SR-548)	10 Business Days
17	Delivery of vulnerability mitigation plan (SR-557)	5 Business Days
18	Delivery of vulnerability mitigation report (SR-575)	20 Business Days
19	Open Incident Ticket (SR-597)	5 minutes
20	Terminate transport across non-domestic links (SR-2)	2 hours

Table 6: Service Level Targets for Contractor Responsibilities

26. Service Migration Phase

26.1. Service Migration Phase Overview

26.1.1. The Service Migration Phase is focused on development and implementation of the systems, processes, tools and reporting required to operate, administer and manage EC MAN/WAN Services.

26.1.2. The Service Migration Phase has two stages:

a) Migration Readiness Stage: During this stage the Contractor must perform all the activities required to develop and implement EC MAN/WAN Services as defined in the subsection entitled Migration Readiness Stage.

b) Migration Stage: During this stage the Contractor must perform all the activities required to migrate EC's SDPs to EC MAN/WAN Services as defined in the subsection entitled Migration Stage.

26.1.3. The Service Migration Phase must begin on the date of Contract award.

26.1.4. During the Service Migration Phase, the Contractor must send weekly written reports to the Technical Authority on the progress of the following:

a) Facility Build progress/completed

b) on-site surveys progress/completed

c) site fit-up in progress/completed

d) network service implementation in progress/completed

e) SDP migrations scheduled/completed

26.1.5. The Contractor must develop an interim service provisioning process in consultation with EC for processing EC MAN/WAN Service Orders until the completion of the Migration Readiness Stage. The interim Service Provisioning process must be modified until approved by EC.

26.1.6. The Contractor must implement the interim service provisioning process until the completion of the Migration Readiness Stage.

26.2. Migration Readiness Stage

26.2.1. The Contractor must provide and receive EC's written acceptance for a migration project schedule for the Migration Readiness Stage of the MAN/WAN migration from the existing EC contract, which includes the completion and acceptance of the following work according to the deliverable time frames identified in the Contract:

a) A **Service Design** that includes:

   i. conceptual design and architecture

   ii. location of Contractor POPs

   iii. logical and physical connectivity topology diagrams that show the network connections between Contractor POPs

   iv. how routing diversity is provided

   v. high-level design for each Transport Circuit by NAP Interface

   vi. list of Contractor Equipment to be located on EC's SDPs (include details on space, weight, power, electrical and environmental requirements)

   vii. a physical representation of the Access Link

   viii. NAPs.

b) **Security High-Level Service Design** – A high-level component diagram that clearly shows the EC MAN Services architecture – including:

   i. allocation of services and components to network security zones and identification of key security-related data flows

   ii. a description of the network zone perimeter defences and, where applicable, a description of the use of virtualization technologies

   iii. descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers

   iv. descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements

   v. allocation of the security requirements at each of the architecture layers of the high-level service design

   vi. definition of the architectural layers (e.g. communications layer, virtualization layer, platform/operating system layer, data management layer, middleware layer, business application layer)

   vii. a description of the approach for remote management, access control, security management and audit, configuration management, and patch management

viii. justification for key design decisions; how the following security functions will be implemented: access control, security management and audit, configuration management, patch management; and remote management

ix. justification for key security design decisions as they relate to network security zoning, network and network zone perimeter defence, and the use of virtualization technology

c) **Security Detailed Service Design Trace** – A subcontract requirements traceability matrix (SRTM) that must include for each security requirement in Appendix C – Statement of Work Security Requirements:

i. the security requirement identifier (SR) from Appendix C – Statement of Work Security Requirements

ii. an identifier that maps the security requirement to the corresponding statement in the SOW (e.g. heading or line identifier) and the security requirement statement from Appendix C – Statement of Work Security Requirements

iii. a description of how the security requirement is addressed in the security detailed-level design in sufficient detail to allow EC to confirm that the security safeguards satisfy the security requirements; the title of the Contract deliverable(s) where the Contractor will provide the details of its security solution for the requirement (e.g., service continuity plan)

iv. tracing (a reference to an identifiable element) to the security detailed-level Service Design to allow EC to confirm that the security safeguards satisfy the security requirements

d) **Security Installation Procedures** – A security installation procedures that must include:

i. steps necessary for the secure installation and configuration of EC MAN and for the secure preparation of the operational environment

ii. installation and configuration of all technical security solutions

iii. security configuration of hardware products and security configuration of software products (commercial off-the-shelf and open source)

e) **Integration Test Plan –** An integration security test plan that must include:

i. the security functions or sets of security functions to be tested, including:

1) a description of the test case, procedure, or scenario
2) environmental requirements
3) ordering dependencies and expected results (i.e. pass/fail criteria)

ii. EC witnessing arrangements

iii. an updated SRTM that contains, for each security requirement to be tested by the integration security test plan, the tracing (a reference to an identifiable element) to integration security testing test cases

f) **Vulnerability Assessment Plan** – A Vulnerability Assessment Plan that must include:

i. a description of the scope of the vulnerability assessment

ii. EC witnessing arrangements

iii. a description of the vulnerability assessment process and of the vulnerability assessment tools that will be used, including any software versions

iv. a description of the test case, procedure, or scenario

v. environmental requirements

vi. ordering dependencies and expected results (i.e. pass/fail criteria)

g) **Operational Security Procedures** – Operational security procedures for each Operator role that must include:

i. schedule of security-relevant actions to be performed in order to maintain the security posture of the EC MAN/WAN Services

ii. how to use available operational interfaces

iii. each scheduled action and how the Operator is expected to perform it

iv. operational roles and responsibilities for:

v. definition of interaction requirements with EC representatives, including:
1) reporting schedule and procedures
2) access control

3) audit and accountability
4) identification and authentication
5) system and communications protection
6) security awareness and training
7) configuration management
8) service continuity and contingency planning
9) risk assessment
10) Incident response
11) maintenance
12) media protection
13) physical and environment protection
14) personnel security
15) system and information integrity

h) **Vulnerability Assessment Report** – Based on a vulnerability assessment conducted in accordance with the vulnerability assessment plan, which necessitates that the Contractor implement patches and corrective measures as part of vulnerability assessment activity, and 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 Service Request Tickets for any required patch or corrective measure that cannot be implemented as part of the vulnerability assessment activity – that includes:

i. a listing of the vulnerability assessment tests that were conducted

ii. for each vulnerability assessment test, each of the following:
    1) whether a known vulnerability was detected
    2) a description of the vulnerability
    3) a description of the patch or corrective measure that was implemented to resolve the vulnerability

iii. for any unresolved vulnerability, at least one of the following:
    1) an assessment of the significance of the vulnerability in the context of the EC MAN Services
    2) the problem ticket number for the outstanding patch or corrective measure
    3) the rationale for not implementing a patch or a corrective measure

i) **Acceptance Test Plan (ATP)** – An ATP for the implementation of a transport circuit (and that the Contractor must modify as requested by EC), that includes:

i. test cases for the verification and validation of the following:
   1) SOW requirements selected by EC
   2) EC MAN/WAN Service is configured per the Service Order

ii. the following information for each test case:
   1) description and objectives of what is to be tested
   2) testing procedures
   3) acceptance criteria and expected results (i.e. pass/fail criteria)
   4) data metrics to be collected and reported

j) **Service Operations Implementation** – The Contractor must implement the requirements in the following subsections according to the accepted Service Design:

i. service desk

ii. Service Portal

iii. Operations Centre

iv. security Operations Centre

v. Contract Management Office

vi. Service monitoring, reporting, and documentation

vii. Information technology service management

viii. billing and invoicing

ix. service provisioning (refer to Service Provisioning, Work Allocation and Access in the Contract)

26.2.2. Implementation Milestones & Remedies

a) The Contractor must meet the following milestones:

i. EC's acceptance of the work performed during the Migration Readiness Stage within 60 Business Days of Contract award

ii. EC's acceptance of the completion of Initial Migration within six months of EC's acceptance of the work performed during the Migration Readiness Stage

b) If the required work associated with either of the two implementation milestones

has not been completed and accepted three months after the original deadline, subject to Excusable Delay, EC may:

i. cancel any existing Service Orders

ii. issue any new Service Orders directly to another contractor

c) If the required work has still not been completed and accepted six months after the original deadline, subject to Excusable Delay, the Parties agree that this constitutes a fundamental breach of the Contract and that EC may:

i. terminate the Contract for default, without providing any further notice or opportunity to cure

ii. cancel any existing Service Orders (including those forming part of initial service project 1 or initial service project 2)

iii. begin issuing or continue issuing any new Service Orders directly to another contractor

26.2.3. Acceptance During Migration Readiness Stage

a) The Contractor must receive EC's acceptance for all deliverables associated with the Migration Readiness Stage as well as acceptance of the completion of the Migration Readiness Stage as a major milestone.

b) EC may, in its sole discretion, agree in writing to extend the delivery time frames for Migration Readiness Stage deliverables and thereby extend the date by which the Contractor must obtain EC's acceptance for any aspect of the work associated with the Migration Readiness Stage. However, any such individual extension does not, in itself, extend the deadline for the completion of Migration Readiness. If EC provides an extension for a specific deliverable, the extension will only apply to that deliverable and not to any other deliverable for the Migration Readiness Stage. Where EC grants an extension for one or more deliverables, and EC accepts the remaining deliverables for the Migration Readiness Stage, the Migration Readiness Stage will be considered to be conditionally accepted for the purpose of moving forward with the Migration Stage. For the deliverables for which any extension has been granted, the Contractor must obtain EC's acceptance by the extended deadline approved by EC for each deliverable.

c) For example, EC agrees to extend acceptance of the ATP for 30 business days beyond the originally scheduled completion date. EC grants conditional acceptance

and proceeds with the Migration Stage. If the Contractor does not obtain EC's acceptance within the 30 business days, Service Credits will apply.

d) With regard to the delivery timeframes associated with security assessment and authorization (SA&A), any delay (i.e. beyond five Business Days) in EC's review and response to Gate 1 deliverables will automatically extend the date for the completion of Gate 2. Any delay in EC's review and response for Gate 2 deliverables will similarly extend the date for the completion of Gate 3. If EC delays review and response for the Contractor's SA&A deliverables, beyond the required completion date for the Migration Readiness Stage, no Service Credits will apply if this delay is the only reason that the Contractor did not complete the Migration Readiness Stage on schedule.

e) The Migration Readiness Stage deliverable schedule provided in Table 7 includes a list of deliverables with acceptance time frame requirements.

Migration Readiness Stage Deliverable Accepted by EC	**Deliverable Time Frame**	**Service Credits**
Project plan for Migration Readiness Stage	20 Business Days after Contract award	Service Credit = $200 per Business Day or partial Business Day late
Project schedule for Migration Readiness Stage	20 Business Days after Contract award	Service Credit = $200 per Business Day or partial Business Day late
Service Design	50 Business Days after Contract award	Service Credit = $200 per Business Day or partial Business Day late
Security assessment and authorization Gate 1	60 Business Days after Contract award	0.5% for each control under the target to a maximum of 5% of the monthly invoice
Service continuity plan	70 Business Days after Contract award	Service Credit = $200 per Business Day or partial Business Day late
Acceptance Test Plan	80 Business Days after Contract award	Service Credit = $200 per Business Day or partial Business Day late
Security assessment and authorization Gate 2	60 Business Days after SA&A Gate 1 acceptance by EC	0.5% for each control under the target to a

		maximum of 5% of the monthly invoice
Security assessment and authorization Gate 3	120 Business Days after SA&A Gate 2 acceptance by EC	0.5% for each control under the target to a maximum of 10% of the monthly invoice
Project plan for Migration Stage	60 Business Days after Contract award	Service Credit = $200 per Business Day or partial Business Day late
Operations readiness	60 Business Days after Contract award	Service Credit = $200 per Business Day or partial Business Day late

Table 7: Migration Readiness Stage Deliverable Schedule

26.3. Migration Stage

26.3.1. The Contractor is responsible for and must manage and coordinate all aspects of the Work required to implement EC MAN/WAN Services including:

a) provision and installation of all Connecting Equipment

b) provision and installation of cable termination equipment such as customer interface panels

c) provision and installation of wall mounting surfaces such as plywood backboards, etc.

d) provision and installation of Contractor Equipment at EC SDPs as rack mounted (default) or shelf mounted when specified by EC in the Service Order

e) conduct of on-site surveys to confirm infrastructure availability and site fit-up requirements including Connecting Equipment, power, space and heating/ventilation/air conditioning (HVAC) within the SDP

f) implementation of the Contractor Equipment within the physical location at the SDP (rack, shelf) as specified by EC; in the event the Contractor Equipment is implemented in the wrong location, the implementation will be considered incomplete until the Contractor returns and relocates the equipment at no cost to EC

g) label of all Contractor Equipment and cables at each SDP using a naming convention specified by EC

h) facilitation of all construction of Connecting Equipment including all administration, procurement and logistics associated with any required fit-up and construction except for power, space and HVAC

26.3.2. EC will specify the Requested Delivery Date (RDD) for each Service Order for each SDP to be migrated.

26.3.3. EC will not issue Service Orders for more than the Maximum SDP Migration Rate unless agreed to by the Contractor.

26.3.4. The Contractor must not perform service migration implementation activities at an EC SDP without prior written approval from the Technical Authority.

26.3.5. EC will be responsible for providing power, space, racks and shelves for Contractor Equipment within an EC SDP.

26.3.6. The Contractor must not locate any of its Contractor Equipment that is used to provide services to any other customer of the Contractor within an EC SDP.

26.3.7. The Contractor must connect the NAP to EC's equipment at SDPs prior to completion of the ATP using the cable provided by the Contractor when requested by EC in the Service Order. EC will provide direction on the equipment and port for the connection.

26.3.8. The Contractor must remain at an SDP until EC confirms that the EC MAN/WAN Service is operational based on evidence provided by the Contractor and the execution of the ATP.

26.3.9. The Contractor must provide all hardware and software for acceptance testing performed by the Contractor. The Contractor must not install nor require EC to install any software on EC's devices to conduct acceptance testing.

26.3.10. EC may require the Work to be performed during or after regular business hours. Business hours vary by SDP based on the nature of business conducted. The Contractor must perform all onsite implementation Work activities according to the time of day specified by EC.

26.3.11. EC may, at its discretion, assume responsibility for implementation of conduit for Inside Cable Plant or may direct the Contractor to use existing conduit. In either case, the Contractor must follow EC's direction to use the existing conduit or to transfer responsibility for the conduit to EC.

26.3.12. Issues that the Contractor encounters that involve third parties, such as building owners and site property managers, do not justify late completion of an

implementation or represent an Excusable Delay pursuant to the General Conditions.

26.3.13. The Contractor must use a parallel cut process to implement EC MAN/WAN Services, where existing equipment and facilities remain in place until the implementation is successfully completed. A flash-cut/hot-cut process must only be used when approved by EC.

26.4. Acceptance Procedures for Initial Migration Service Orders and Start of Billing

26.4.1. For Service Orders that are part of Initial Migration, the acceptance procedures will be as follows:

a) EC will specify the Requested Delivery Date in each Service Order that it issues for Initial Migration.

b) Once the Contractor has implemented a Service Order, the Contractor must send EC a Work Completion Notice (WCN) and an Acceptance Test Report (ATR) based on the approved ATP for that Service Order. The ATR must confirm positive results of ATP execution.

c) EC must migrate the Service at the SDP specified in the WCN within five Business Days of the Requested Delivery Date in the Service Order or within five Business Days of receiving the WCN – whichever is later.

d) Once EC has migrated to that Service at the SDP, a 10 Business Day Acceptance Period will apply. During the 10 Business Day Acceptance Period, as part of EC's acceptance process for a Service, EC may test any function of the Service to determine whether it meets the requirements of the Contract. If the Service does not meet the requirements of the Contract, EC may reject the Work or require that it be corrected at the Contractor's expense before accepting the Work. No payments for the Service are chargeable under the Contract until the Service is accepted.

e) If EC provides notice of any deficiency during the 10 Business Day Acceptance Period by initiating an Incident Ticket, the Contractor must address the deficiency at no cost to EC as soon as possible, notify EC in writing once the deficiency is corrected and re-issue the WCN, at which time EC will be entitled to re-inspect the Work and the 10 Business Day Acceptance Period will start again.

f) At 11:59 p.m. (ET) on the final day of the 10 Business Day Acceptance Period during which EC has not initiated any Incident Ticket, EC will be deemed to have accepted the Service. The Contractor may begin billing for the Service effective the

day following that acceptance.

g) The acceptance procedures for the Service Orders completed as part of Initial Migration can be illustrated by the following examples:

Example 1:

i. the RDD for a Service is April 15, 2017

ii. the Contractor provides the WCN on April 11, 2017

iii. EC migrates to that Service on April 15, 2017

iv. no Incident Ticket is issued for the Service during the 10 Business Day Acceptance Period

v. the Contractor bills for that Service beginning effective April 30, 2017 (the 11th Business Day after April 15, 2017)

Example 2:

i. the RDD e for a Service is June 15, 2017

ii. the Contractor provides the WCN on June 10, 2017

iii. EC migrates to that Service on June 15, 2017

iv. an Incident Ticket for an outage to the Service is initiated on June 21, 2017

v. the 10 business day Acceptance Period is reset and begins on June 22, 2017 (the next business day after June 21, 2015)

vi. no further Incident Tickets are initiated for the Service during the restarted 10 Business Day Acceptance Period

vii. the Contractor bills for that Service beginning effective July 8, 2015 (the 11th Business Day after June 22,2015)

26.5. Acceptance Procedures for Service Orders and Start of Billing After Initial Migration

26.5.1. For all other Service Orders (i.e. any Service Order not forming part of Initial Migration), the acceptance procedures will be as follows:

a) As set out in the service provisioning process, each Service Order will be issued by EC with an RDD. Once the Contractor has implemented a Service, the Contractor must send EC a WCN and an ATR based on the approved ATP for that Service.

b) On the day that EC receives the WCN and ATR, or the RDD – whichever is later – EC will be deemed to have accepted the Service and the Contractor may begin billing for the Service. However, if EC migrates to the Service before the RDD, the Contractor may begin billing on the Business Day immediately following the day on which the migration takes place.

c) The WCN must state that the Work has been fully inspected and tested in accordance with the approved ATP.

d) An ATR must contain the following information for each of the test items in the associated ATP:

   i. the expected results (i.e. pass/fail criteria)

   ii. the actual results

   iii. a description of deviations and how each was resolved

   iv. a traceability matrix that describes how each requirement (including reports, data, service levels and documentation) of the work in the ATP was tested and validated (i.e. demonstration, documentation, etc.)

   v. the SLT testing results

e) The Contractor must assist EC with the analysis, isolation and correction of problems detected during EC's acceptance testing.

27. Transition Services / Contract Close-Out Phase

27.1. Contract Close-Out Phase

27.1.1. In the period leading up to the end of the Contract Period, also referred to as the Contract Close-Out Phase, the Contractor will make all reasonable efforts to assist EC in the transition from the Contract to a new contract with another supplier or to EC itself. The Contractor agrees that there will be no charge for these transition services.

27.1.2. The following applies with respect to these transition services:

a) The Contract Close-Out Phase may overlap with the implementation phase of any

follow-on contract issued by EC.

b) EC may issue one or more Service Order and/or Service Request for the Contract Close-Out Phase.

c) During the Contract Period, the Contractor must continue to provide the MAN/WAN Services until the MAN/WAN Services are terminated during the transition to the follow-on contractor or to EC itself.

d) The Contractor, upon receiving notification of EC initiated Contract termination or the expiration of the contract term, must work with EC to effect a seamless transition of MAN/WAN Services from the Contractor to the follow-on contractor or to EC – whichever will be performing the same or similar work. In doing so, the Contractor agrees to work closely and co-operatively with the follow-on contractor(s) or EC at no additional cost.

e) As part of the transition services, within 30 Business Days of a request by EC, the Contractor must provide operational, administrative, management, support, maintenance, technical, design, configuration, network diagrams and schematics, naming and addressing information and documentation for all the MAN/WAN Services in an electronic file format and file naming convention specified by EC.

f) The Contractor must request from EC, no later than 60 Business Days before the Contract expiration date, disposal instructions for the MAN/WAN Services data. The Contractor must return and/or dispose of its MAN/WAN Services data holdings in accordance with the instructions provided by EC and perform media sanitization in compliance with CSE ITSG-06. Upon request by the Technical Authority, the Contractor must provide a certification that it has disposed of the MAN/WAN Services Data in accordance with this Contract.

28. Service Credits

28.1. Migration Stage

28.1.1. The SLTs and associated Service Credits for service provisioning will not apply to the migration of the IBIS NAPs that are defined in the Service Catalogue or those that are added to the Service Catalogue from existing contracts listed in the Pricing Commitment. However, EC may use the SDIs for service provisioning as a guide in its estimation of the migration schedule.

28.1.2. New SDPs that are added to the Service Catalogue after Contract Award, and which are

not defined in an existing contract listed in the Pricing Commitment, are not considered to be part of the Migration Stage and must:

a) be implemented in parallel to Migration SDPs in accordance with the SLTs for service provisioning

b) not impact the Maximum SDP Migration Rate and the project schedule for the Migration Stage.

28.1.3. If the Contractor fails to successfully migrate one or more Migration SDPs for the IBIS by the RDD during the Migration Stage, Service Credits will apply according to the following provisions:

a) For each of the first five Migration SDPs that the Contractor fails to successfully migrate by the RDD in a month, the Contractor must provide EC with a Service Credit of $2,500. For example, if the Contractor fails to migrate three Migration SDPs in a month by their respective RDDs, the Contractor must provide EC with a Service Credit of $7,500

b) For each Migration SDP exceeding the quantity of five that the Contractor fails to successfully migrate by the RDD in a month, the Contractor must provide EC with a Service Credit of $5,000. For example, if the Contractor fails to migrate a total of eight Migration SDPs in a month by their respective RDDs, the Contractor must provide EC with a total Service Credit of $27,500 (5 x $2,500 + 3 x $5,000)

c) In any given month, any Migration SDP that was not successfully migrated by the RDD during a previous month, and is still not successfully migrated during the current month, will be subject to a Service Credit of $5,000, regardless of the number of failed SDP migrations that month. These Service Credits will continue to accrue each month until the SDP has been successfully migrated; however, the Migration SDPs with RDDs in previous months that have still not been successfully migrated will not be counted for the purpose of determining how many Migration SDPs the Contractor failed to successfully migrate in the current month

28.1.4. SLTs will not apply during the 10-Business Day Acceptance Period for SDP migrations during Initial Migration. For example, the SLT-MTRS will not apply if the service fails in the first 10 Business Days following the migration of the Migration SDP.

28.1.5. SDP migrations that take place after Initial Migration will not be subject to the 10-Business Day Acceptance Period. SLTs for those services will apply immediately following their migration.

28.2. Failure to Meet Service Level Target for Service Availability

28.2.1. If the Contractor fails to meet the SLT-SA for an IBIS NAP in any given month, the Contractor must provide a Service Credit to EC, as summarized in Table 8.

SLT-SA		Service Credit for SLT-SA Exceptions
SA	99.90%	Applies to failures of the single NAP for single Access Link Service Credit for first occurrence in any 12-month period = CMP for NAP x 100% Service Credit for second occurrence in any 12-month period for the same NAP = CMP for NAP x 150% Service Credit for third and subsequent occurrences in any 12-month period for the same NAP = CMP for NAP x 200%

Table 8: Service Credits for SLT-SA Exceptions

28.3. Failure to Meet Service Level Target for MAN/WAN Aggregate Availability

28.3.1. If the Contractor fails to meet the SLT for MAN/WAN Aggregate Availability (SLT-WAA), the Contractor must provide a Service Credit to EC equal to 20% of the total combined CMP for all IBIS NAPs that were in service during the month in which the SLT-WAA exception occurred, regardless of whether all IBIS NAPs were affected.

28.4. Failure to Meet Service Level Target for Maximum Time to Restore Service

28.4.1. If the Contractor fails to meet the SLT-MTRS at any time for any IBIS NAP, then the Contractor must provide a Service Credit to EC as set out in Table 9.

28.4.2. The maximum total Service Credit that can apply for an SLT-MTRS exception is the CMP for the affected NAP times 200%.

SLT-MTRS		Service Credit for SLT-MTRS Exceptions
MTRS during an Electoral Event period	1 hour	Service Credit for NAP service outage > 1 and < 2 hours = CMP for NAP x 100% An additional CMP x 25% for each additional 1-hour interval (or part thereof) of NAP service outage time starting at 3 hours Example 1: Service Credit for 3 hours = CMP x 125% Example 2: Service Credit for 4.5 hours = CMP x 150%

MTRS during a non-Electoral Event period	4 hours	Service Credit for NAP service outage > 4 and < 6 hours = CMP for NAP x 100% An additional CMP x 25% for each additional 2-hour interval (or part thereof) of NAP service outage time starting at 6 hours Example 1: Service Credit for 6 hours = CMP x 125% Example 2: Service Credit for 9 hours = CMP x 150%

Table 9: Service Credits for SLT-MTRS Exceptions

28.5. Failure to Meet Service Level Target for Service Portal Maximum Time to Restore

28.5.1. If the Contractor fails to meet the SLT-SPMTR at any time, then the Contractor must provide a Service Credit to EC of $5,000. For each additional day of Service Portal outage time for the critical functions of Incident Tickets, Service Orders or ad hoc and on-demand reports, the Contractor must provide EC with an additional Service Credit of $5,000. For each additional day of Service Portal outage time for any other function (i.e. other than Incident Tickets, Service Orders or ad hoc and on-demand reports), the Contractor must provide EC with an additional Service Credit of $5,000.

28.5.2. If the Contractor fails to meet the SLT-SPMTR three or more times in any 12-month period, the Service Credit payable to EC for the third and each subsequent individual occurrence in the same 12-month period will automatically double.

28.6. Failure to Meet Service Level Targets for Packet Transit Delay, Packet Loss Ratio, and Packet Delay Variation

28.6.1. If the Contractor fails to meet the Service Level Targets for packet transit delay (SLT-PTD) and/or packet delay variation (SLT-PDV) in a calendar month, the Contractor must provide a Service Credit to EC as set out in Table 10.

Failed Packet Streams per Month	Service Credit for SLT-PTD and SLT-PDV Exceptions (applies to the NAP in the pair with the lowest CMP)
11 – 26	Service Credit = NAP with the lowest CMP x 25%
27 – 43	Service Credit = NAP with the lowest CMP x 50%

> 43	Service Credit = NAP with the lowest CMP x 100%

Table 10: Service Credits for SLT-PTD and SLT-PDV Exceptions

28.6.2. If the Contractor fails to meet the SLTs for packet transit packet loss ratio (SLT-PLR) in a calendar month, the Contractor must provide a Service Credit to EC as set out in Table 11.

SLT-PLR	Traffic Classes (Class of Service [CoS])	Packet Loss Ratio per Month	Service Credit for SLT-PLR Exceptions (applies to the NAP in the pair with the lowest CMP)
SLT-PLR	CoS-2, CoS-3	>0.5% ≤ 0.7%	Service Credit = NAP with the lowest CMP x 25%
		>0.7% ≤ 0.9%	Service Credit = NAP with the lowest CMP x 50%
		>0.9%	Service Credit = NAP with the lowest CMP x 100%
	CoS-4, CoS-5	>0.05% ≤ 0.10%	Service Credit = NAP with the lowest CMP x 25%
		>0.10% ≤ 0.20%	Service Credit = NAP with the lowest CMP x 50%
		>0.20%	Service Credit = NAP with the lowest CMP x 100%

Table 11: Service Credits for SLT-PLR Exceptions

28.6.3. If the Contractor fails to meet a SLT-PTD, and/or SLT-PLR, and/or SLT-PDV for the same class of service for the same virtual private network (VPN) in a calendar month, it will be counted as a single SLT exception for the purpose of determining the Service Credit the Contractor must provide to EC. In the case where there are multiple SLT exceptions for the same class of service for the same VPN in a calendar month, the worst SLT exception must be used to determine the amount of Service Credit.

28.6.4. The total sum of Service Credits for SLT exceptions associated with any individual NAP-to-NAP performance measurement in a month cannot exceed 100% of the lowest CMP in the pair of NAPs.

28.7. Failure to Meet Service Level Target for Service Desk Response

28.7.1. If the Contractor fails to meet the SLT-SDR in a calendar month, the Contractor must provide a Service Credit to EC of $5,000.

28.7.2. If the Contractor fails to meet the SLT-SDR three or more times in any 12-month period, the Contractor must provide an additional Service Credit to EC of $20,000 (i.e. total of $25,000) for the third and every subsequent occurrence in the same 12-month period.

28.8. Failure to Meet Service Level Targets for Service Provisioning

28.8.1. If the Contractor fails to meet the SLT-SP, the Contractor must provide a Service Credit to EC as set out in Table 12.

28.8.2. The Service Credit for an SLT-SP exception accumulates each Business Day that the Contractor is late in completing the Work. The Service Credit is calculated using either a fixed dollar amount or a percentage of the CMP (for the affected NAP). In some cases, the unit used for calculation of the Service Credit is determined by the one with the greatest value. For example, if the CMP x 10% is $500, it will be used to calculate the Service Credit because it is greater than the fixed amount of $300.

28.8.3. The Service Credit for an SLT-SP exception cannot exceed the CMP x 200% for the affected NAP. The exception to this is Service Credits associated with Request for Unscheduled Work Estimate Responses, where the maximum is $5,000.

	SLT-SP Description	SDI	Service Credit (amount per Business Day late)
1	Implement a change to the committed traffic rate (CTR) for an existing IBIS NAP where the Access Link is already installed, operational, and with capacity	5 Business Days	Service Credit = $100
2	Replace an IBIS NAP with another IBIS NAP (i.e. different NAP ID)	20 Business Days	Service Credit = greater of $200 or NAP CMP x 10%
3	Implement an IBIS NAP and single Access Link where the Access Link exists and there is sufficient capacity for the required CTR	30 Business Days	Service Credit = greater of $300 or NAP CMP x 10%

4	Implement IBIS NAPs and dual Access Links where the Access Links exist for the required CTR (sufficient capacity on existing access facilities)	40 Business Days	Service Credit = greater of $300 or NAP CMP x 10%
5	Implement an IBIS NAP and single Access Link and Dual Access Links where a Facility Build is required	65 Business Days	Service Credit = greater of $300 or NAP CMP x 10%
6	Implement IBIS NAPs and dual Access Links where a Facility Build is required	80 Business Days	Service Credit = greater of $300 or NAP CMP x 10%
7	Provide a Request for Unscheduled Work Estimate Response for New SDP	20 Business Days	Service Credit = $200
8	Provide a Request for Unscheduled Work Estimate Response for CTR, SLT-SA, SLT-MTRS and dual access of an Existing SDP	10 Business Days	Service Credit = $200
9	Provide detailed description supporting Request for Unscheduled Work Estimate Response	20 Business Days	Service Credit = $200

Table 12: Service Credits for SLT-SP Exceptions

28.9. Failure to Meet Service Level Targets for Service Delivery Response

28.9.1. If the Contractor fails to meet the SLT-SDRES, the Contractor must provide a Service Credit to EC as set out in Table 13.

	SLT-SDRES Description	SDI	Service Credit
1	Service Portal administration: changes to access profiles, User accounts, role-based access controls	2 Business Days	Service Credit = $500
2	Reset a User account password on the Service Portal	4 hours	Service Credit = $500
3	Configuration of an access control list for a NAP	4 hours	Service Credit = $500
4	Disable/enable a NAP	1 hour	Service Credit = $500

5	Posting of weekly reports on Service Portal	2 Business Days	Service Credit = $200 per Business Day or partial Business Day late
6	Posting of monthly reports on Service Portal	5 Business Days	Service Credit = $200 per Business Day or partial Business Day late
7	Posting of semi-annual reports on Service Portal	10 Business Days	Service Credit = $500 per week or partial week late
8	Posting of annual reports on Service Portal	30 Business Days	Service Credit = $500 per week or partial week late
9	Delivery of post-Incident Request reports	2 Business Days	Service Credit = $200 per Business Day or partial Business Day late
10	Delivery of post-Service Request reports	5 Business Days	Service Credit = $200 per Business Day or partial Business Day late
11	Delivery of Security Incident post-mortem report (SR-606)	72 hours	Service Credit = $500 per Business Day or partial Business Day late
12	Notification Security Operations Centre not available (SR-580)	15 minutes	Service Credit = $500 per hour or partial hour late
13	Provide security Operations Centre acknowledgement of received e-mail (SR-584)	15 minutes	Service Credit = $500 per hour or partial hour late
14	Invoice and supporting documentation	5 Business Days	Service Credit = $200 per Business Day or partial Business Day late
15	Response to request for archived information	5 Business Days	Service Credit = $200 per Business Day or partial Business Day late
16	Initiation of Service Request (per EC's request)	1 Business Day	Service Credit = $200 per Business Day or partial Business Day late
17	Update to documentation and data repositories	10 Business Days	Service Credit = $200 per Business Day or partial Business Day late
18	Configuration Management Database (CMDB) updates	5 Business Day	Service Credit = $100 per Business Day or partial Business Day late
20	Update to Service Design document	20 Business Days	Service Credit = $200 per Business Day or partial Business Day late

21	Configuration change to existing NAP for measurement of SLT-PTD/PLR/PDV	2 Business Days	Service Credit = $200
22	High-level security Incident assessment	8 hours	Service Credit = $500 per hour or partial hour late
23	Detailed-level security Incident assessment	2 Business Days	Service Credit = $500 per Business Day or partial Business Day late

Table 13: Service Credits for SLT-SDRES Exceptions

28.10. Failure to Meet Security Requirements Implementation

28.10.1. Security requirements implementation progress is the measure of the number of controls met by the Contractor at specified milestone dates. Table 14 describes the security requirements implementation progress service level metric.

28.10.2. At each gate identified in Table 14, the Contractor will be measured on their compliance with the security requirements found in Appendix C – SOW Security Requirements. The SLT for each gate is shown in Table 14.

	SLT-Security Requirements	SDI	Service Credit (amount per month late)
1	Gate 1 – 75% of the controls	Within 60 business days of Contract award	0.5% for each control under the target to a maximum of 5% of the monthly invoice
2	Gate 2 – 90% of the controls	Within 120 business days of Contract award	0.5% for each control under the target to a maximum of 5% of the monthly invoice
3	Gate 3 – 100% of the controls	Within 240 business days of Contract award	0.5% for each control under the target to a maximum of 10% of the monthly invoice

Table 14: Service Credits for Security Requirements Implementation

28.11. Contractor Failure to Perform its Responsibilities

28.11.1. The SLT-CONRES represent a partial description of the Contractor's Work responsibilities and is not a complete listing of the Contractor's responsibilities or obligations as defined in the Contract. In addition to the Contractor responsibilities listed for SLT-CONRES, EC has the right to require the Contractor to undertake the remedial action described in this sub-section entitled Contractor Failure to Perform its Responsibilities, for the Contractor's failure to perform any of its responsibilities associated with delivery of the EC MAN/WAN Services as defined in the Contract and for which there is no other remedial action defined.

28.11.2. The process for requiring the Contractor to undertake remedial action if the Contractor fails to meet the SLT-CONRES, or for any other Contractor responsibility defined in the Contract but not addressed elsewhere in this section will be as follows:

a) EC will notify the Contractor in writing (e.g. e-mail) that a failure to meet a SLT-CONRES has occurred. EC will provide specific details regarding the failure.

b) The Contractor must respond to EC within three Business Days with an action plan to resolve the failure for EC's approval. The Contractor's action plan must demonstrate how the failure will be resolved within one month of the notification from EC. The Contractor must add the failure to the agenda and action item log for the related monthly service management meeting.

c) If the Contractor fails to deliver an action plan, or if in EC's opinion the Contractor has failed to resolve the failure according to the approved action plan within the one-month period, EC will notify the Contractor in writing a second time. In the second notification, EC will provide the new target date for the Contractor's resolution of the failure.

d) If in EC's opinion the Contractor has failed to resolve the failure within the revised target date, then remedial action automatically becomes applicable on the Business Day after the target date.

28.11.3. The Contractor must provide EC with a Service Credit of $1,000 for each Business Day or partial Business Day the failure is not resolved beyond the first one-month period or revised target date.

28.11.4. Some of the Contractor's responsibilities are one-time obligations or infrequent, such as the delivery of test results to EC within 10 Business Days of completion of the annual service continuity plan testing. In cases where the failure related to

performance of its responsibilities is for an infrequent activity, the Contractor's plan must demonstrate it is committed to ensuring the failure is not repeated. EC's acceptance of the Contractor's action plan may in itself constitute resolution of the failure, as determined by EC. However, if following acceptance of the Contractor's action plan, the failure is then repeated, EC may immediately require remedial action. In such cases, the Contractor must provide a Service Credit to EC of $2,000 each time the failure recurs.

28.11.5. Service Credits are cumulative and can apply concurrently for different SLT exceptions and/or failures by the Contractor to perform its responsibilities as defined above.

28.12. Contractor Failure to Implement Internet Protocol Version 6

28.12.1. If the Contractor fails to implement IPv6 routing, the Contractor must provide a Service Credit to EC equal to $5,000 for each month of delay (and pro-rated for any partial month), which becomes due on the first Business Day of each month following December 31, 2017, until the Contractor implements native routing of IPv6 traffic.

28.13. Service Credit Calculation

28.13.1. The Contractor must calculate Service Credits based on its performance of the Work against the SLTs for the previous month beginning on the first day of each monthly billing cycle and ending on the last day of that billing cycle.

28.14. Service Credit Cap

28.14.1. The maximum total sum of Service Credits that can apply in any calendar month for SLT exceptions is 20% of the Contractor's total invoice for Services in that month (not including applicable taxes). There are two exceptions to this, which are the Service Credits associated with:

a) the Migration Readiness Stage

b) the Migration Stage

28.14.2. Service Credits associated with the activities in these two stages will be separate and in addition to any other Service Credits applicable for SLT exceptions. For example, in the event that the Contractor missed the RDD for several SDP migrations in a month, the Service Credits owed to EC would not be counted towards the Service Credit Cap.

28.15. Chronic Service Level Conditions

28.15.1. The following each constitute a Chronic Service Level Condition:

a) an SLT-MTRS exception occurs for the same NAP at the same SDP more than three times in any rolling three-month period following Contract award

b) an SLT-SA exception occurs for the same NAP at the same SDP more than three times in any rolling six-month period following Contract award

c) an SLT-PTD, SLT-PLR or SLT-PDV exception occurs for the same NAP at the same SDP more than three times in any rolling six-month period following Contract award

28.15.2. If a Service is subject to a Chronic Service Level Condition, EC may cancel the affected Service and issue a Service Order to another contractor to replace it.

28.16. Contract Termination for Cause

28.16.1. The Contractor will be deemed to be in Default of the Contract and subject to the terms of the General Conditions Services – Default by the Contractor, should any of the following occur:

a) three or more network outages of two hours or more, on any or all segments of the network, within a 30-day period

b) Network Availability standards are not met for three months within any six-month time frame

29. Dispute Resolution

29.1.1. Any dispute concerning this Contract that cannot be resolved by discussions or written communications between the Contracting Authority and the Contractor's service manager within 20 business days will be handled as follows:

a) After the 20-Business-Day-period, either Party may give notice to the other containing a request to negotiate, which must contain a description of the nature of the dispute and any relevant background details and refer to specific articles of the Contract that relate to the dispute. The Party receiving the request to negotiate must provide the request to negotiate to:

i. in the case of EC, to the Director, IT Infrastructure Operations

ii. in the case of the Contractor, a sales director, an individual who is not involved in the day-to-day administration of the Contract and is someone who corresponds to the director level within the Contractor's organization

b) Within 10 Business Days of receiving a request to negotiate, the receiving Party must respond in writing with its position regarding the nature of the dispute, any additional relevant details and any additional articles of the Contract that Party considers relevant to the dispute. The Party receiving this response must provide the response to:

   i. in the case of the EC, to the Director, IT Infrastructure Operations

   ii. in the case of the Contractor, to a sales director, an individual not involved in the day-to-day administration of the Contract and who corresponds to the Director level within the Contractor's organization

c) If the dispute is not resolved within 10 Business Days of the response being provided, the Parties agree to refer the matter to the following individuals, depending on the nature of the dispute:

   i. If the dispute concerns a financial matter not exceeding $1 million or the delivery of goods and services for which payment would not exceed $1 million:

      1) in the case of the EC, to the Chief Information Officer

      2) in the case of the Contractor, to a vice president, an individual who is not involved in the day-to-day administration of the Contract and who corresponds to the director general level within the Contractor's organization

   ii. For all other matters,

      1) in the case of the EC, to a deputy chief electoral office

      2) in the case of the Contractor, to a vice president, individual not involved in day-to-day administration of the Contract and who corresponds to an assistant deputy minister level within the Contractor's organization

d) The Parties agree that negotiations will begin between these individuals within 10 business days. However, negotiations need not necessarily take place in the form of a face-to-face meeting.

e) Either Party may choose to bring the dispute to a more senior individual in its own organization at any time.

f) If the dispute is not resolved through these negotiations within a total of 60 Business Days (including all of the above steps), the Parties agree to consider referring the matter to more senior officials in their respective organizations and/or to consider other appropriate dispute resolution processes before resorting to litigation.

29.1.2. All information exchanged during these negotiations or other dispute resolution processes will be regarded as “without prejudice” communications for the purpose of settlement negotiations and will be treated as confidential by the Parties and their representatives, unless otherwise required by law. However, evidence that is independently admissible or discoverable will not be rendered inadmissible or non-discoverable by virtue of its use during the negotiations or other alternate dispute resolution process.

29.1.3. A Contract dispute is defined as any disagreement that cannot be resolved at a contract management review meeting.

Metropolitan Area Network and Wide Area Network Services

Appendix A

Glossary of Terms and Acronyms

(draft)

Term	Definition
10 Business Day Acceptance Period	Has the meaning ascribed to it in Section 26.4.1(d) of the SOW.
30 Victoria	EC headquarters located at 30 Victoria Street, Gatineau, Quebec.
150 Tunney's Pasture	EC office located at 150 Tunney's Pasture Driveway, Ottawa, Ontario.
440 Coventry	EC warehouse located at 440 Coventry Road, Ottawa, Ontario.
Acceptance Period	The time period for EC to conduct acceptance testing for a Service Order following receipt of the Work Completion Notice (WCN).
Acceptance Test Plan (ATP)	A document that describes the tests the Contractor must perform on the Work before submitting it to EC for acceptance or delivery.
Acceptance Test Report (ATR)	A document that describes the results of the acceptance testing according to the Acceptance Test Plan.
Access Area	The Entrance Link and Equipment Area designated by EC for a building or campus where a SDP is located.
Access Link	The Contractor Equipment and Connecting Equipment between a Contractor Point of Presence (POP) and an SDP.
Access Profile	A grouping of role-based access controls for Service Portal accounts.
Access Network	All Access Links that connect to the Core Network.
Administrator	A User who is authorized to perform administrative operations for the EC MAN/WAN Services.
Authentication	A process to verify the digital identity of the sender of a network communication.
Billing Detail File	A file that contains billing records.
Boundary Protection	A managed interface between Network Security Zones that controls and monitors the flow of data by applying defined security policies. Examples include proxies, gateways, routers, firewalls, guards, or encrypted tunnels.
EC LAN	LAN infrastructure located at an EC SDP.
EC SDP	SDP designated by EC.
EC SIEM	The SIEM located in the EC MAN/WAN Services Security Operations Zone.
EC Wide Area Network (WAN)	Wide Area Network (WAN) services provided by EC and/or SSC.
CEA	The *Canada Elections Act,* S.C. 2000, c. 9, as amended from time to time.
CEO	The Chief Electoral Officer of Canada.
Chronic Service Level Condition	Has the meaning ascribed to it in Section 28.15 of the SOW.
Circuit	A physical connection on which information is transmitted.
Circuit Rate	The sustained full duplex bandwidth throughput of a Transport Circuit.
Classified Information	Relates to the national interests of Canada. It concerns the defence and maintenance of the social, political, and economic stability of

Term	Definition
	Canada. There are three levels of classified information: 1) Top Secret: a very limited amount of compromised information could cause exceptionally grave injury to the National Interest; 2) Secret: compromise could cause serious injury to the National Interest; and 3) Confidential: compromise could cause limited injury to the National Interest.
Client Data	Data that is transported between NAPs by EC MAN/WAN Services.
Committed Delivery Date (CDD)	Date by which the Contractor has committed to successfully complete a Service Order.
Computing Infrastructure	Computer hardware, software and firmware components (e.g. desktop computers, laptop computers, servers, electronic storage, printers, operating system software and application software).
Configuration Item (CI)	Any hardware and/or software component or asset used to provide EC MAN/WAN Services.
Configuration Management	Standardized methods and procedures for managing changes made to Configuration Items.
Configuration Management Data Base (CMDB)	A database used to store information about Configuration Items (CIs) and their relationships with other CIs throughout their lifecycle.
Committed Traffic Rate (CTR)	The sustained full duplex bandwidth throughput of an IBIS NAP.
Connecting Equipment	Includes the Inside Cable Plant and Outside Cable Plant.
Contractor Equipment	Hardware and software components provided by the Contractor for an EC MAN/WAN Service that are located at an Equipment Area or SDP.
Contractor OAM Infrastructure	Hardware and software components used by the Contractor for its operation, administration and/or management (OAM) of EC MAN/WAN Services, excluding any component that requires access to the EC MAN/WAN Services Internetwork Operational Configuration.
Contractor OAM Zone	Restricted Zone or Management Restricted Zone where Contractor operation, administration and management (OAM) activities for the Core Network, Access Network (excluding Contractor Equipment) and Contractor OAM Infrastructure are conducted.
Contractor Point Of Presence (POP)	A Contractor Service Delivery Point (SDP).
Contractor Service Delivery Point (SDP)	An SDP designated by the Contractor where EC MAN/WAN Service Infrastructure is located (not an EC SDP).
Contractor Security Incident Data	Incident Ticket data for Security Incidents associated with the Contractor Security Operations Zone, Contractor OAM Infrastructure,

Term	Definition
	Core Network and Access Network (excluding Contractor Equipment).
Contractor Security Operations	Contractor operation, administration and management for SIEM Infrastructure, Security Incident investigations, host-based intrusion and prevention systems, AV/AS and malware protection systems, audit logs and analysis, Boundary Protection systems, vulnerability monitoring and analysis activities performed by the Contractor in the Contractor Security Operations Zone, Contractor OAM Zone, Core Network and Access Network (excluding Contractor Equipment).
Contractor Security Operations Zone	A Restricted Zone or Management Restricted Zone where Contractor Security Operations are conducted at a Contractor SDP.
Contractor SIEM	The SIEM located in the Contractor Security Operations Zone.
Core Network	Hardware and software for EC MAN/WAN Services that interconnects Contractor POPs and terminates Access Networks.
Customer Edge (CE) Router	A router owned, operated, administered, managed and implemented by the Contractor at an EC SDP that provides an IBIS NAP.
Customer Router	A router located at an EC SDP that is owned and operated by EC.
Cyber Event	An attack, damage or unauthorized access of networks, computers, programs and data.
Data Centre	A facility used to house computer systems and associated components, such as telecommunications and storage systems.
Denial of Service	An attempt to make a machine or network resource unavailable to its intended users.
Dynamic Host Configuration Protocol (DHCP) Relay Agent	A device that is configured to listen for DHCP or BOOTP broadcasts from DHCP clients and then relay those messages to DHCP servers.
Digital Private Line NAP	A NAP type for Digital Private Line Circuits.
Digital Private Line Circuit	A dedicated point-to-point or multi-point connection between 2 or more Digital Private Line NAPs that transports data, voice and video on a dedicated transport circuit.
Direct Material Cost	Actual cost of the material necessary to construct the Connecting Equipment for a Facility Build, without any markup (whether for profit, overhead, or otherwise).
Domain	A logical grouping of Services that share a business or technical affinity such as type of service, trust relationship, technical authority, etc.
EC	The Office of the CEO, commonly known as Elections Canada.
Election Day	The final date for voting in an Electoral Event.
Electoral Event	General elections, by-elections, and federally organized referendums. The CEA states that an Electoral Event must last a minimum of 36 days. For the purpose of this SOW, an Electoral Event commences when the writ is issued and concludes on Election Day.

Term	Definition
Emergency Service Request	A Service Request for an EC MAN/WAN Service that must be implemented on an expedited basis to address urgent changes. For example: address a critical Incident impacting Users or implement an urgent change to contain and mitigate a Security Incident.
Enhancement	An upgrade or improvement to a software application; often referred to as an "interim release", which is often documented by adding a further decimal and digit to the version or release number (i.e., V.X.X.2 would be the next enhancement after V.X.X.1).
Entrance Link	The physical path for Outside Cable Plant to enter a building designated by EC.
Equipment Area	A physical location in a building designated by EC for Contractor Equipment.
Event and Incident Management	The standardized methods and procedures to restore a Service to normal operation as quickly as possible, and to minimize the impact on EC business operations.
Existing Circuit	A Circuit defined in the Service Catalogue.
Existing SDP	An SDP that is defined in the Service Catalogue.
Facility Build	All work required to implement Connecting Equipment, including materials and services and anything else required to complete the work.
EC MAN/WAN Services	Includes Layer 2 and Layer 3 (MPLS) Inter-Building Internetwork Service (IBIS).
EC MAN/WAN Services Data	EC MAN/WAN Services Security Data, EC MAN/WAN Services SDP Device Configuration Data, EC MAN/WAN Services System Data, and EC MAN/WAN Services OAM Data on any media.
EC MAN/WAN Services Infrastructure	Contractor Equipment and hardware and software components that are used for EC MAN/WAN Services Security Operations and EC MAN/WAN Services Network Operations
EC MAN/WAN Services Contractor Infrastructure	Contractor OAM Infrastructure and hardware and software components provided and managed by the Contractor that process EC Data, excluding Internetwork Components provided and managed by Contractor subcontractors.
EC MAN/WAN Services Network Operations	Contractor operation, administration and management of EC MAN/WAN Services Internetwork Operational Configuration.
EC MAN/WAN Services Security Infrastructure	Computing Infrastructure and Internetwork Components used by the Contractor associated with EC SIEM Infrastructure, host-based intrusion and prevention systems, AV/AS and malware protection systems and Boundary Protection systems.
EC MAN/WAN Services Internetwork Operational Configuration	The set of Contractor-configured commands that customize the functionality of Contractor Equipment that operate with an IP/Layer 3 configuration to deliver EC MAN/WAN Services.

Term	Definition
EC MAN/WAN Services OAM Data	Data that the Contractor uses for the operation, administration and management (OAM) of EC MAN/WAN Services including: Service Requests, Problem Tickets, Incident Tickets (excluding Security Incident Tickets), Service Orders, Billing Detail Files, invoices, CMDB records (excluding the IP/Layer 3 Operational Configuration of applicable Contractor Equipment), capacity planning and network performance data and reports.
EC MAN/WAN Services SDP Device Configuration Data	Electronically-stored copies of the EC MAN/WAN Services Internetwork Operational Configuration.
EC MAN/WAN Services Security Data	The EC MAN/WAN Services Security Incident Data and EC MAN/WAN Services Security Operations Data.
EC MAN/WAN Services Security Incident Data	Incident Ticket data for Security Incidents associated with the EC MAN/WAN Services Security Operations Zone, EC MAN/WAN Services Network Operations Zone, and Contractor Equipment.
EC MAN/WAN Services Security Operations Data	Data for EC SIEM Infrastructure, Security Incident investigations, host-based intrusion and prevention systems, AV/AS and malware protection systems, audit logs and analysis, Boundary Protection systems, vulnerability monitoring and analysis.
EC MAN/WAN Services Security Operations	Operation, administration and management activities performed by the Contractor for EC SIEM Infrastructure, Security Incident investigations, host-based intrusion and prevention systems, AV/AS and malware protection systems, audit logs and analysis, Boundary Protection systems, vulnerability monitoring and analysis. Applies to the EC MAN/WAN Services Security Operations Zone, EC MAN/WAN Services Network Operations Zone and Contractor Equipment.
EC MAN/WAN Services Security Operations Zone	Restricted Zone or Management Restricted Zone dedicated to EC where EC MAN/WAN Services Security Operations are conducted.
EC MAN/WAN Services Network Operations Zone	Restricted Zone or Management Restricted Zone dedicated to EC where EC MAN/WAN Services Network Operations are conducted.
EC MAN/WAN Services System Data	Data related to diagrams, documents and reports for EC MAN/WAN Services.
Hardware	All the equipment, materials, matters and things used by the Contractor to provide the EC MAN/WAN Service to EC under the Contract (including cables and other ancillary items), including firmware, if any, but not including software or services.
Incident	An event that is not part of the standard operation of the EC MAN/WAN Services and that causes, or may cause, an interruption to, or a reduction in, the quality of the EC MAN/WAN Services (including all

Term	Definition
	operations, management and administration systems, including the Service Portal).
Incident Ticket	A record describing an Incident.
Information Breach	The intentional or unintentional release of secure information to an untrusted environment. Examples include: information leaking, transmission of classified information on non-classified systems, and privacy breach.
Inside Cable Plant	The cabling (copper and fiber), connectors, conduit, ducts, repeaters, and other equipment to connect the Contractor Equipment in the Equipment Area to the Contractor Equipment at the SDP in the Telecom Room.
Internet	Collection of interconnected networks and application servers that are publicly accessible worldwide and that are commonly referred to as the Internet.
Inter-Building Internetwork Service (IBIS)	An EC MAN/WAN Service, owned and managed by the Contractor.
Internetwork Components	Hardware and software components of EC MAN/WAN Services that are accessible (read or write) using the Internet Protocol (IP).
Internet Protocol Security (IPsec)	A network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys for use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.
Jitter	The variation in latency as measured in the variability over time across a network.
Key Performance Indicator (KPI)	A measure of the performance of a Service.
Key Resources	A resource provided by the Contractor as identified in the Contract.
King Edward Datacentre (KED)	The main EC datacentre located at 350 King Edward Avenue in Ottawa that serves as the hub for the EC MAN and any future WAN connectivity.
Known Error	Identified root cause of a Problem.
Latency	The total time taken for a network unit of data to travel from source (i.e. one NAP) to destination (i.e. another NAP) one way. This total time is the sum of both the processing and serialization delays in the network

Term	Definition
	elements and the propagation delay along the transmission medium.
Local Area Network (LAN)	Supplies networking capability to a group of computers in close proximity to each other.
Malware	Short form for malicious (or malevolent) software. Used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software.
Management Restricted Zone	A Restricted Zone established by the Contractor for management of EC MAN/WAN Services Infrastructure.
Markup Rate	The maximum percentage markup for the costs of any work (services and products) for a Facility Build.
Maximum SDP Migration Rate	The maximum number of Migrated SDPs that EC can require implementation/migration in any month during the Migration Stage.
Metropolitan Area Network (MAN)	A metropolitan area network (MAN) is a computer network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network).
Migration SDPs	Existing SDPs or New SDPs that are listed in the Service Catalogue Unmanaged MAN Table.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Examples of mobile code technologies include Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.
Mobile Device	A tablet, cellular phone, smart phone or other similar portable telecommunications device.
Mobile Network	Public network for mobile devices.
Multiprotocol Label Switching (MPLS)	A type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence its name "multiprotocol". MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL.
National Capital Region (NCR)	The area that comprises the greater Ottawa-Gatineau metropolitan area.
Network Access Point	One or more NAP Interfaces at an EC SDP used to interconnect EC and

Term	Definition
(NAP)	provider networks.
Network Access Point Identifier (NAPID)	A unique alphanumeric identifier for a NAP.
NAP Interface	A physical and logical point of attachment of Contractor Equipment to EC's equipment at an EC SDP.
NAP Interface Identifier (NAPINID)	A unique alphanumeric identifier for a NAP Interface.
NAP Interface Rate	The sustained full duplex data transfer rate for a Network Interface.
NAP Type	A type of Network Access Points.
Network Availability	The service metric for the time during which packets on all network segments can be successfully sent and received between KED and any MAN connected buildings.
Network Interface	The point of interconnection between networks and other networks or computers
Network Security Zone	An Operations Zone, Public Access Zone, Restricted Zone or Management Restricted Zone.
New Release	A system release, a version release, or interim release of software used by the Contractor to provide the EC MAN/WAN Services, regardless of whether the Contractor refers to it as a "new release".
New SDP	An SDP that is not defined in the Service Catalogue.
Operations Centre	The Contractor location where infrastructure required for the centralized management and operation of the EC MAN/WAN Services is installed.
Operator	A Contractor resource that administers EC MAN/WAN Services Infrastructure or processes EC MAN/WAN Services OAM Data.
Original Equipment Manufacturer (OEM)	The manufacturer of an item of Hardware, as evidenced by the name appearing on the hardware and on all accompanying documentation.
Operations Zone	Common network operating environment for daily business operations.
Outside Cable Plant	The cabling (copper and fiber), connectors, conduit, ducts, poles, towers, repeaters, antennae and other equipment used to interconnect the Contractor Equipment at the Contractor POP to the Contractor Equipment at the Access Area in a building or campus.
Packet Delay Variation	A KPI that is a measure of the time difference between successive data packets received between two NAPs.
Packet Loss	A KPI that is the number of packets lost between two NAPs over a fixed time period.
Physically Diverse	Describes the separate physical equipment and facilities that must be provided in order to achieve redundancy among separate Access Links. For an Access Link to be Physically Diverse from another Access Link to the same SDP, the entrance to the building, the conduits, the cooper/fiber facilities, the Contractor Equipment, etc. must all be physically separate. For greater certainty, but without limitation,

Term	Definition
	physical diversity cannot be achieved using virtual means; using different cables in the same conduit; using a single entrance to EC's building; or using a single entrance to the Contractor's POP.
Portable Digital Media	A form of electronic removable media (e.g. a USB key, a USB hard drive, a memory stick, etc.) where data are stored in digital form, which can be easily transported from place to place.
Power Condition	Describes an issue or problem with the power supporting EC MAN/WAN Services, including complete failure of power, reduced power (brownout) and low battery of power backup equipment.
Power over Ethernet (PoE)	Describes any of several standardized or ad-hoc systems which pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as wireless access points, IP cameras, and VoIP phones.
Privacy Breach	Incident involving the unauthorized disclosure of personal information.
Problem	Unknown cause of one or more Incidents often identified as a result of multiple similar Incidents.
Problem Management	The standardized methods and procedures to proactively prevent Incidents from happening, minimize the impacts of Incidents that cannot be prevented and minimize the impact of Problems for EC MAN/WAN Services.
Problem Ticket	A record describing a Problem.
Protected Information	This refers to information that the Government of Canada treats as protected and confidential, including the following information: a) Protected A (low-sensitive): Applies to information that, if compromised, could reasonably be expected to cause injury outside the National Interest (e.g. disclosure of exact salary figures). b) Protected B (particularly sensitive): applies to information that, if compromised, could reasonably be expected to cause serious injury outside the National Interest (e.g. loss of reputation or competitive advantage). c) Protected C (extremely sensitive): applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the National Interest (e.g. loss of life).
Provider Edge (PE) Router	A router at a Contractor POP in the Core Network that connects to a CE router.
Public Access Zone	A tightly controlled environment that protects internal networks and

Term	Definition
	applications from a hostile public zone, such as the Internet.
Public Key Infrastructure (PKI)	Infrastructure that binds the publically available encryption and signing keys with their registered users or devices by means of a certificate authority.
Remote Access	Access to the EC MAN/WAN Services Infrastructure through an external network (e.g. the Internet).
Remote Management	Administrative or maintenance activities conducted by an operator over a network.
Request Fulfillment	Standardized methods and procedures used for efficient and prompt handling of all changes to EC MAN/WAN Services, in order to minimize the number and impact of any related changes regarding a Service Request.
Restricted Zone	A controlled network environment for business-critical IT services or large repositories of sensitive information.
Security Incident	A Cyber Event that causes, or may cause, a compromise of the EC MAN/WAN Services' confidentiality, integrity, or availability.
Security Incident Ticket	Record describing a Security Incident.
Security Information and Event Management (SIEM)	A technology that provides real-time analysis (collection, aggregation, correlation) of security alerts generated by infrastructure components and applications.
SIEM Infrastructure	The Computing Infrastructure and Internetwork Components required to provide a SIEM.
Security Posture	A characteristic of an information system that represents the ability of implemented security controls to satisfy the business needs for security and counter a selected threat.
Service	An EC MAN/WAN Service that can be ordered by EC from the Service Catalogue.
Service Catalogue	The list of Service Catalogue Identifiers and Service Catalogue Items.
Service Catalogue Identifier (SCID)	A unique identifier of a Service Catalogue Item.
Service Catalogue Item (SCI)	An element of an EC MAN/WAN Service that can be ordered by EC with a Service Order.
Service Credit	A fee that the Contractor must pay or credit to EC upon failure to meet a specific obligation under the Contract.
Service Credit Cap	Has the meaning ascribed to it in Section 28.14 of the SOW.
Service Degradation	Incident whereby the quality of EC MAN/WAN Services being delivered is impacted. EC MAN/WAN Services may still be available but the full performance levels required of the EC MAN/WAN Services are not being met.
Service Delivery Interval (SDI)	The maximum amount of time for the Contractor to complete Work.

Term	Definition
Service Delivery Point (SDP)	Physical location in a building for 1 or more NAPs.
Service Delivery Point Identifier (SDPID)	A unique alpha-numeric identifier for an SDP.
Service Design	The contractor's design of EC MAN/WAN Services.
Service Level Target (SLT)	A performance value determined by EC for the Contractor's delivery of the EC MAN/WAN Service, and for which the Contractor must conduct measurements and reporting. The Contractor's failure to meet or exceed an SLT may result in remedial action.
Service Order	A request from EC for the purchase of a Service Catalogue Item from the Service Catalogue.
Service Order Period	The total number of months, including any partial months, between the date that the Service Order is transmitted to the Contractor and the end date specified in the Service Order.
Service Portal	A specially designed website that brings together all information related to the services being provided to EC.
Service Portal Account	A User account on the Service Portal.
Service Portal Zone	Public Access Zone to protect the Service Portal connection to the Internet.
Service Releases	A release of software that is designed to operate on designated combinations of computer hardware and operating systems. A new Service Release typically will be indicated by the addition of one (1) to the first digit of the release number (i.e., v.2.X.X would be the next Service Release after v.1.X.X).
Service Request	A request to make a change to EC MAN/WAN Services.
Service Request Acknowledgement Notice	A notice sent to EC when a Service Request is received from EC.
Service Request Implementation Notice	A notice sent to EC when a Service Request is ready for implementation.
Service Request Cancellation Notice	A notice sent to EC when a Service Request is cancelled.
Service Request Completion Notice	A notice sent to EC when a Service Request is completed.
Service Request Ticket	A record describing a Service Request.
Social Engineering	The manipulation of people into performing actions or divulging confidential information; examples include phishing, whaling, and clone phishing.
Shared Services	EC's partner in delivering central GC network connectivity.

Term	Definition
Canada (SSC)	
Shared Metropolitan Area Network (SMS)	SSC owned MAN service serving the NCR.
Software Patches	An engineering fix to a problem that may be incorporated into a New Release to update software in order to improve or correct errors or defects in the program code.
System	A generic term used to mean network and other devices, operating systems, computing platforms, virtualization software and applications or any combination thereof. Its use is context-specific.
Target Delivery Date (TDD)	Date proposed by the Contractor to complete a Service Order.
Telecommunication Room	Physical location in a building for an SDP.
Threat Vector	A path or a tool that a hacker uses to gain access to a computer or network server in order to deliver a malicious outcome.
Traffic Flow	A sequence of packets that have characteristics in common (e.g. source IP address, destination IP address, port number and type).
Unauthorized Access	Occurs when an entity gains unauthorized access to a system in order to commit another crime, such as destroying information contained in that system; examples include infiltration, compromise, hacking, privilege escalation and unauthorized access/privilege.
User	A person that is authorized to engage in service management activities related to EC MAN/WAN Services.
Virtual Private Network (VPN)	A logical network connection.
Virtual Route and Forwarding (VRF)	A technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.
Voice over IP (VoIP)	A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).
Vulnerability Assessment Report	A report detailing vulnerabilities assessed and tested as part of the vulnerability assessment plan.
Web Browser Client	A mobile or desktop web browser that connects to the EC MAN/WAN Services using HTTP/HTTPS.
Work Completion Notice	The Contractor's certification that the Work has been inspected and tested by the Contractor in accordance with the Acceptance Test Plan

Term	Definition
	(ATP) and is ready for use by EC.

Metropolitan Area Network and Wide Area Network Services

Class of Service

(draft)

Service Class	Application (Examples)	DSCP PHB Set	DSCP Decimal	Traffic Class
Network Control	Network Routing (OSPF, BGP,I-BGP,HSRP,IKE)	CS6	48	CoS-5
Interactive Inelastic Real-Time Services	IP Telephony Signalling (AS SIP, SIP) Command & Control	CS5	40	CoS-5
	IP Telephony media (RTP, SRTP)	EF	46	CoS-5
Responsive Real-Time Services	Multimedia Conferencing (e.g. Telepresence, Boardroom video conferencing)	AF41 AF42 AF43	34 36 38	CoS-4
	Desktop Communications (e.g. WebRTC)	CS4	32	CoS-4
Timely Preferred Elastic Services	Multimedia Streaming (Playback / on demand)	AF31 AF32 AF33	26 28 30	CoS-3
	Broadcast Video (e.g. Live events, surveillance)	CS3	24	CoS-3
	Low-Latency Data (e.g. Instant Messaging, Chat, Presence, ERP, Database)	AF21 AF22 AF23	18 20 22	CoS-3
	Operations, Administration and Management	CS2	16	CoS-3
Best Effort Elastic Services	High Throughput Data	AF11 AF12 AF13	10 12 14	CoS-2
	Standard (e.g. Internet Web)	CS0	0	CoS-2
Scavenger Services	Low Priority Data (without bandwidth assurance)	CS1	8	CoS-1

Metropolitan Area Network and Wide Area Network Services

Statement of Work Security Requirements

(draft)

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Data Security	Data Sovereignty	SR-1	The Core Network and Access Network must reside within Canada, with the exception of emergency situations where Canada authorizes the use of non-domestic connections.	**Examine:** Operational Artefacts - location of data center, storage facilities for off-site media storage	Compliance	No	
Data Security	Data Sovereignty	SR-2	The Contractor must ensure that Client Data traffic initiated in one part of Canada to a destination located in another part of Canada is routed exclusively through Canada, with the exception of emergency situations where a failure occurs in the EC MAN/WAN Service and traffic between SDPs cannot be routed exclusively through Canada. The Contractor must continuously monitor Contractor Core Network infrastructure that provide non-domestic connections and must initiate a Security Incident Ticket if E C 's network traffic is transported across non-domestic connections. The Contractor must terminate transport of Client Data across non-domestic connections within 2 hours of a request by EC.	**Examine:** Development/Installation Artefacts - EC MAN/WAN Services system design documentation, Contractor Core Network configuration/settings details, Contractor Core Network routing information; **Examine:** Operational Artefacts - Procedures for managing network routing; Service arrangements with 3rd parties; Security Incident management; **Test:** ST&E test results to demonstrate the routing details on the EC MAN/WAN Services traffic.	Compliance	No	
Data Security	Data Protection	SR-4	The Contractor must ensure that any EC MAN/WAN Services Data is created and stored on Contractor Computing Infrastructure that is located exclusively in Canada, regardless of the media. The Contractor must ensure that any sessions for Remote Management, EC MAN/WAN Services SDP Device Configuration Data and a EC MAN/WAN Services Internetwork Operational Configuration transmitted electronically across any network is encrypted using cryptographic solutions approved by EC (see SR-20). The Contractor must ensure that any information or data related to the Work, regardless of the media, are physically transported exclusively within Canada.	**Examine:** Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services components; **Examine:** Operational Artefacts - Procedures; **Test:** ST&E test results associated with data protection requirement for EC MAN/WAN Services.	Compliance	No	
Data Security	Data Protection	SR-5	Syslog traffic created by Contractor Equipment must be encrypted using cryptographic solutions approved by EC (see SR-20).	**Examine:** Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services Contractor Equipment; Examine: Operational Artefacts - Procedures; Test: ST&E test results associated with data protection requirement for EC MAN/WAN Services.	Compliance	No	
Data Security	Data Isolation	SR-8	Contractor Equipment at an EC SDP must be physically dedicated to EC's use.	Examine: Development/Integration Artefacts - EC MAN/WAN Services system design documentation, physical hosting location details; facility and system access detail procedures; Interview: Contractor personnel assigned the administrator/operator roles and Contractor personnel responsible for EC MAN/WAN Services.	Compliance	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Encryption	SR-20	The Contractor must ensure that cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for EC MAN/WAN Services: a) use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSEC and validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSA-11E (http://www.cse-cst.gc.ca/its- sti/publications/itsa-asti/itsa11e-eng.html) or in a subsequent version; and b) be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (http://www.cse-cst.gc.ca/its-sti/services/industry-prog- industrie/cmvp-pvmc-eng.html) to at least FIPS 140-2 validation at Level 1.	Examine: EC MAN/WAN Services System and communications protection policy; procedures addressing use of cryptography; CMVP cryptography standards; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.	Compliance, Reliability, Effectiveness	No	
Infrastructure	Authentication	SR-31	Before any route or label exchange occurs between Internetwork Components, the Internetwork Components must confirm a valid peering relationship exists by performing mutual authentication using a Hash-based Message Authentication Code (HMAC) that is derived from either the MD5, SHA-1, SHA-256, SHA-384 or SHA-512 secure hash algorithms.	Examine: secure SDLC artefacts - Access control policy; procedures addressing EC MAN/WAN Services information flow enforcement; procedures addressing source and destination domain identification and authentication, and information transfer error handling; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; other relevant documents or records; Test: ST&E test results that demonstrate the automated mechanisms implementing information flow enforcement policy.	Effectiveness, Reliability	No	
Infrastructure	DoS Protection	SR-61	The Contractor must provide protection against Denial of Service for: a) Service Portal Zone; b) EC MAN/WAN Services Security Operations Zone; c) EC MAN/WAN Services Network Operations Zone; d) Contractor Security Operations Zone; and e) Contractor OAM Zone. (see SR-100)	Examine: secure SDLC artefacts - EC MAN/WAN Services system policies and procedures addressing Denial of Service capability; design documentation; configuration settings; Test: ST&E test results demonstrating compliance to SR-61 requirements.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Acceptable Use - Logon Banner	SR-90	The EC MAN/WAN Services Service Portal must display an acceptable use logon banner approved by EC on the login page of any web-based application for Users. <SR- 90>	Examine: Operational Artefacts - Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of EC MAN/WAN Services system use notification messages or banners; EC MAN/WAN Services system notification messages; EC MAN/WAN Services system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; Test: ST&E results related to EC MAN/WAN Services Service Infrastructure mechanisms implementing the access control policy for system	Completeness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Boundary Protection and Zoning	SR-100	The Contractor must implement the following Network Security Zones: <SR-100> a) EC MAN/WAN Services Network Operations Zone; b) EC MAN/WAN Services Security Operations Zone; c) Contractor OAM Zone; d) Contractor Security Operations Zone; and e) Service Portal Zone. Communication between Network Security Zones must be mediated by Boundary Protection in accordance with the Security Detailed Service Design approved by EC and in compliance with SR-106.	Examine: Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services system including firewalls; Examine: Operational Artefacts - Procedures, Firewalls, routers policy management; Test: ST&E test results associated with network zoning requirement for EC MAN/WAN Services.	Compliance, Effectiveness, Reliability	No	
Infrastructure	Boundary Protection and Zoning	SR-101	The EC MAN/WAN Services Network Operations Zone must exclusively: a) include the EC MAN/WAN Services Network Operations Centre; b) include encrypted storage of EC MAN/WAN Services SDP Device Configuration Data, on storage media physically dedicated to EC; c) include Operator consoles from which Remote Management of a EC MAN/WAN Services Internetwork Operational Configuration must be performed; d) provide Operator access and Computing Infrastructure access to a EC MAN/WAN Services Internetwork Operational Configuration and the EC MAN/WAN Services SDP Device Configuration Data; and e) include a network, physically dedicated to EC use, for interconnection of the zone components.	Examine: Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services system including firewalls; Examine: Operational Artefacts - Procedures, Firewalls, routers policy management; Interview: Contractor personnel with network management responsibilities; Test: ST&E test results associated with network zoning requirement for EC MAN/WAN Services.	Compliance, Effectiveness, Reliability	No	
Infrastructure	Boundary Protection and Zoning	SR-102	The EC MAN/WAN Services Security Operations Zone must exclusively: a) include the EC MAN/WAN Services Security Operations Centre; b) include the EC SIEM system with encrypted storage of EC MAN/WAN Services Security Operations Data on storage media physically dedicated to EC; c) include encrypted storage of EC MAN/WAN Services Security Incident Data on storage media physically dedicated to EC; d) Operator consoles from which Remote Management of EC MAN/WAN Services Security Infrastructure and audit log reviews of EC MAN/WAN Services Security Data must be performed; e) allow access to EC MAN/WAN Services Security Data; and f) include a network, physically dedicated to EC use, for interconnection of the zone components.	Examine: Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services system including firewalls; Examine: Operational Artefacts - Procedures, Firewalls, routers policy management; Interview: Contractor personnel with security operations responsibilities; Test: ST&E test results associated with network zoning requirement for EC MAN/WAN Services.	Compliance, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Boundary Protection and Zoning	SR-103	Unless otherwise approved by Canada, the Contractor OAM Zone must include: a) storage of EC MAN/WAN Services OAM Data and EC MAN/WAN Services System Data that is logically separated from the data of any other Contractor clients; b) Computing Infrastructure for the EC MAN/WAN Services Service Desk; c) Computing Infrastructure for the EC MAN/WAN Services Service Portal; d) Computing Infrastructure used for the management of the Contractor OAM Zone; and e) a dedicated network for interconnection of the zone components.	Examine: Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services system including firewalls; Examine: Operational Artefacts - Procedures, Firewalls, routers policy management; Interview: Contractor personnel with EC MAN/WAN Services OAM responsibilities; Test: ST&E test results associated with network zoning requirement for EC MAN/WAN Services.	Compliance, Effectiveness, Reliability	No	
Infrastructure	Boundary Protection and Zoning	SR-104	The Contractor Security Operations Zone must include: a) Computing Infrastructure for the Contractor SIEM system; b) operator consoles from which Contractor Security Operations are conducted; c) Computing Infrastructure used for the management of the Contractor Security Operations Zone; and d) a dedicated network for interconnection of the zone components.	Examine: Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services system including firewalls; Examine: Operational Artefacts - Procedures, Firewalls, routers policy management; Interview: Contractor personnel with security operations responsibilities; Test: ST&E test results associated with network zoning requirement for EC MAN/WAN Services.	Compliance, Effectiveness, Reliability	No	
Infrastructure	Boundary Protection and Zoning	SR-105	The Contractor must provide a Service Portal Zone.	Examine: Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services system including firewalls; Examine: Operational Artefacts - Procedures, Firewalls, routers policy management; Test: ST&E test results associated with network zoning requirement for EC MAN/WAN Services.	Compliance, Effectiveness, Reliability	No	
Infrastructure	Boundary Protection and Zoning	SR-106	Operator consoles within the EC MAN/WAN Services Network Operations Zone and the EC MAN/WAN Services Security Operations Zone: a) must have no Internet access except as defined in SR- 107; b) must not have access to the Contractor's corporate applications, including but not limited to instant messaging, VoIP and videoconferencing; c) may send/receive email to/from the gc.ca. Internet domain related to the provision of EC MAN/WAN services; d) may have access to the Contractor's corporate service for DNS and Operator Identification and Authorization, and other corporate services as approved by EC during the Contract.	Examine: Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services system including firewalls; Examine: Operational Artefacts - Procedures, Firewalls, routers policy management; Interview: Contractor personnel with boundary protection responsibilities; Test: ST&E test results associated with network zoning requirement for EC MAN/WAN Services.	Compliance, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Boundary Protection and Zoning	SR-107	Connections to suppliers in support of product updates, patches and signature files, within the EC MAN/WAN Services Network Operations Zone and the EC MAN/WAN Services Security Operations Zone, must: a) be conducted through a secure proxy or application- aware firewall limited by source and destination rules specified by EC, in compliance with SR-178; b) be limited to protocols approved by EC; and c) be initiated from within the EC MAN/WAN Services Network Operations Zone/EC MAN/WAN Services Security Operations Zone.	Examine: Development/Installation Artefacts - Detailed Design document, configuration settings for EC MAN/WAN Services system including firewalls; Examine: Operational Artefacts - Procedures, Firewalls, routers policy management; Interview: Contractor personnel with boundary protection responsibilities; Test: ST&E test results associated with network zoning requirement for EC MAN/WAN Services.	Compliance, Effectiveness, Reliability	No	
Infrastructure	Boundary Protection and Zoning	SR-108	The Contractor must provide Contractor SIEM evidence of any Contractor Security Operations Zone, Contractor OAM Zone, Contractor Core Network and Contractor Access Network (excluding Contractor Equipment) components compromised by a cyber attack. The Contractor must provide EC SIEM evidence of any EC MAN/WAN Services Security Operations Zone, EC MAN/WAN Services Network Operations Zone and Contractor Equipment components compromised by a cyber attack, and from the Contractor SIEM in compliance with SR-594. The Contractor must initiate a Security Incident Ticket upon detection of a cyber attack that includes: a) denial of service attacks; b) unauthorized intrusion or access; c) social engineering; d) malware; and information breach.	Examine: Operational Artefacts - EC MAN/WAN Services system and communications protection policy; procedures addressing boundary protection; communications and network traffic monitoring logs; other relevant documents or records; Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; boundary protection hardware and software; EC MAN/WAN Services system architecture and configuration documentation; EC MAN/WAN Services system configuration settings and associated documentation; Interview: Contractor/SSC personnel with boundary protection responsibilities; Test: ST&E test results associated with interfaces implementing EC MAN/WAN Services traffic flow policy.	Completeness, Effectiveness, Reliability	No	
Security Operations	Logging and Auditing	SR-113	The Contractor must provide evidence associated with a Security Incident, based upon criteria specified by EC, within 72 hours, that includes: <SR-113> a) results of logs and audit records research; and b) results of SOC Operator analysis of logs and audit records.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Authentication	Logging and Auditing	SR-115	The EC MAN/WAN Services must log the following information for all Operator and Administrator activities: a) Operator/Administrator identifier; b) date and time stamp of the activity; c) description of the activity performed; and d) data modified by the activity.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	
Security Operations	Logging and Auditing	SR-189	The EC SIEM must aggregate and correlate event and audit logs captured by EC MAN/WAN Services Security Operations, and from Contractor Security Operations in compliance with SR-594. The EC MAN/WAN Services SOC Operator must conduct investigations of SIEM data with the following data management functions: a) viewing; b) searching; c) filtering; d) sorting: e) exporting, f) archiving; g) generating reports; h) analysis. The Contractor must allow EC's IPC to conduct investigations using EC SIEM data with the following data management functions via the SOC-to-IPC connection, in compliance with SR-192: a) viewing; b) searching; c) filtering; d) sorting: e) exporting, f) archiving; g) generating reports; and h) analysis. Two-factor authentication in compliance with SR-292 must be used for any access to EC MAN/WAN Services Security Data.	Examine: Operational Artefacts - System and information integrity policy; procedures addressing EC MAN/WAN Services system monitoring tools and techniques; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system monitoring tools and techniques documentation; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system protocols documentation; Examine: Operational Artefacts - Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation, EC MAN/WAN Services system audit records; audit tools; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services ST&E result supporting near real-time event analysis, mechanisms implementing audit information protection, mechanisms implementing non- repudiation capability, and media storage devices to hold audit records.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Logging and Auditing	SR-190	The Contractor SIEM and EC SIEM must: a) include centralized and time-synchronised logging of allowed and blocked change activity; b) daily log analysis of change activity; c) retain the last 3 months of events and logs online; d) retain the last 2 years of events and logs associated with a Security Incident; e) store logs for at least 1 year; and f) support categorization of events and logs based on selectable filters.	Examine: Operational Artefacts - System and information integrity policy; procedures addressing EC MAN/WAN Services system monitoring tools and techniques; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system monitoring tools and techniques documentation; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system protocols documentation; Examine: Operational Artefacts - Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation, EC MAN/WAN Services system audit records; audit tools; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services ST&E result supporting near real-time event analysis, mechanisms implementing audit information protection, mechanisms implementing non- repudiation capability, and media storage devices to hold audit records.	Completeness, Effectiveness, Reliability	No	
Security Operations	Logging and Auditing	SR-192	The Contractor must provide an encrypted (in compliance with SR-20) electronic feed of the dataset from the EC SIEM to EC's IPC in a protocol approved by EC, according to a frequency, data format and dataset/subset specified by EC. The Contractor must ensure that EC's IPC can decrypt the received dataset. <SR-192> EC will provide the network connection between the EC MAN/WAN Services SOC and EC's IPC. <SR-192> The Contractor must provide EC with a minimum of 10 User accounts with read-only access to the EC MAN/WAN Services Security Data accessible using the network connection to the EC MAN/WAN Services SOC. The User accounts must be protected by two-factor authentication in compliance with SR-292. <SR-192>	Examine: Operational Artefacts - Procedures addressing audit information copy to SSC, Logs of transfer; Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation, EC MAN/WAN Services system audit/logging records; audit tools; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services ST&E result supporting mechanisms implemented for copy of events in specific format.	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Continuous Monitoring	Vulnerability Assessment	SR-545	The Contractor must allow EC, or its representatives, to conduct a non-disruptive/non-destructive vulnerability assessment of the Internetwork Components of Contractor Equipment and the Service Portal within 3 Business Days of a request by EC, that includes: < SR-545> a) network access to the Internetwork Components of Contractor Equipment and the Service Portal to allow for authenticated and unauthenticated scanning using EC-operated equipment, and EC-specified tools; and b) assistance for the duration of any on-site portion of the vulnerability assessment of at least one technical resource that is familiar with the technical aspects of the EC MAN/WAN Services Contractor Infrastructure (i.e., the hardware, software, and network components, security appliances, and their configuration).	Examine: Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Continuous Monitoring	Vulnerability Management	SR-546	The Contractor must: <SR-546> a) report any security issue for EC MAN/WAN Services as a Security Incident immediately upon learning of its existence; b) track identified Security Incidents; and c) report daily progress of Security Incidents to EC, until each Security Incident is fixed or mitigated.	Examine: Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Continuous Monitoring	Vulnerability Management	SR-547	The Contractor must correct all security issues and deficiencies at no additional cost to EC as identified through:<SR-547> a) EC security audits and vulnerability assessments; b) the Contractor's own continuous security monitoring activities; and c) the Original Equipment Manufacturer's security monitoring activities for EC MAN/WAN Service hardware and software.	Examine: secure SDLC artefacts - EC MAN/WAN Services system risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records. Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.		Yes	
Continuous Monitoring	Vulnerability Management	SR-548	The Contractor must mitigate a security vulnerability identified in a Security Incident according to a mitigation plan approved by EC as follows: a) high-risk vulnerabilities within 10 Business Days of EC's approval of the mitigation plan; and b) moderate risk vulnerabilities within 30 Business Days days of EC's approval of the mitigation plan. <SR-548> The Contractor will assign a risk rating of vulnerabilities using the Common Vulnerabilities Scoring System (CVSS) v2 and as approved by EC. <SR-548> The Contractor must adopt updated CVSS versions during the Contract Period within 6 months of release. <SR-548>	Examine: secure SDLC artefacts - EC MAN/WAN Services system risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records. Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.		Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Continuous Monitoring	Authorization Maintenance	SR-550	The Contractor must continuously monitor the implemented security requirements to determine if the security of the EC MAN/WAN Services Infrastructure continues to be effective. <SR-550> The Contractor must perform an annual audit of the implemented security requirements to determine if the security of the EC MAN/WAN Services Infrastructure continues to be effective. <SR-550> The Contractor must provide evidence on the effectiveness of the maintenance of security authorization for EC MAN/WAN Services within 30 Business Days of a request by EC. <SR-550>	Examine: Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Continuous Monitoring	Authorization Maintenance	SR-552	The Contractor must update security operating procedures for the security authorization of EC MAN/WAN Services within 30 Business Days of a request by EC. <SR-552> The Contractor must submit an annual revision of the Operational Security Procedures document for EC's approval not more than 20 Business Days after the Contract anniversary date. <SR-552>	Examine: Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Continuous Monitoring	Continuous Monitoring	SR-554	The Contractor must maintain the Security Posture of EC MAN/WAN Services by continuously monitoring for: <SR-554> a) threats and vulnerabilities; and b) malicious activities and unauthorized access. The Contractor must take proactive countermeasures for EC MAN/WAN Services that include: <SR-554> a) pre-emptive and response actions to mitigate threats; b) notifying EC of any countermeasure actions implemented; and c) removing the countermeasures as directed by EC.	Examine: Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Continuous Monitoring	Vulnerability Management	SR-557	The Contractor must provide a vulnerability mitigation plan, for approval by EC, within 5 Business Days of completion of a vulnerability assessment, that includes proposed protection measures to mitigate the risks identified from the vulnerability assessment or to satisfy the EC MAN/WAN Services security requirements. <SR- 557>	Examine: Operational Artefacts - change logs, Implementation details; supporting documentation as required	Compliance, Completeness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Configuration Management	Change Management	SR-560	All Service Requests that may disrupt EC MAN/WAN Services must be approved by EC. <SR-560>	Examine: secure SDLC phases - Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the EC MAN/WAN Services system; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system architecture and configuration documentation; other relevant documents or records; Interview: Contractor personnel with configuration change control responsibilities; Test: ST&E test result related to demonstrate mechanisms implementing baseline configuration maintenance.	Completeness, Effectiveness, Reliability	Yes	
Service Continuity	Contingency Planning	SR-571	The Service Continuity Plan must include: <SR-571> a) a detailed plan and documented processes for restoring EC MAN/WAN Services; b) detailed communications plans with EC, EC's Clients and the Contractor's suppliers and sub-contractors; c) a detailed plan and processes for transferring operational, management and administration functionality to a backup operations centre; d) a detailed plan and processes for transferring operational, management and administration functionality to a backup Service Desk; e) back up strategies for network facilities, operational support systems and data, key service components and EC MAN/WAN Services Data; f) how the Contractor will ensure that its sub-Contractors have service continuity plans in place; g) description of the process for testing the service continuity plan; h) the steps the Contractor will take if any of its key subcontractors and/or suppliers go out of business, and i) the steps the Contractor will take if a manufacturer or Original Equipment Manufacturer (OEM) of infrastructure components used to deliver EC MAN/WAN Services is identified by EC as being subject to security concerns. The Contractor must implement the Service Continuity Plan (all processes, procedures, roles, responsibilities etc) within 60 Business Days following its acceptance by EC. < SR-571>	Examine: Contingency planning policy; procedures addressing contingency operations for the EC MAN/WAN Services system; contingency plan; security plan; business impact assessment; other relevant documents or records; Interview: Contractor personnel with contingency planning and plan implementation responsibilities; Contractor personnel with incident handling responsibilities.	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Continuous Monitoring	Patch Management	SR-572	The Contractor must provide patch management for the EC MAN/WAN Services Infrastructure that includes: <SR- 572> a) ensuring the latest version of software is used within Computing Infrastructure and Internetwork Components; b) ensuring that vulnerabilities are evaluated and vendor- supplied security patches are applied in a timely manner; c) coordinating completion of patch management activities with its third-party suppliers in a timely manner; d) prioritizing critical patches using a risk-based approach; e) taking applications offline and bringing them back online f) aligning the criticality levels for patches as specified by EC; g) rating vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2; h) using a testing and verification methodology to ensure that patches have been implemented properly.	Examine: secure SDLC artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; Examine: Operational Artefacts - patch and vulnerability management records; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records; Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Continuous Monitoring	Vulnerability Assessment	SR-574	The Contractor must automatically scan for vulnerabilities on the EC MAN/WAN Services Service Portal on a monthly basis and as requested by EC. <SR-574> The Contractor must provide EC with a copy of the vulnerability scanning report of the EC MAN/WAN Services Service Portal within 5 Business Days of completion of the scan. <SR-574>	Examine: secure SDLC artefacts - EC MAN/WAN Services system risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and EC MAN/WAN Services system components checked; other relevant documents or records.		Yes	
Continuous Monitoring	Vulnerability Management	SR-575	The Contractor must provide a vulnerability mitigation report to EC within 20 Business Days after completion of remediation activities performed in compliance with SR- 547, that includes: <SR-575> a) a description of the corrective measures implemented; and b) proof that associated system documentation has been updated to reflect the changes.	Examine: secure SDLC artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; Examine: Operational Artefacts - patch and vulnerability management records; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records; Interview: Contractor personnel with risk assessment and vulnerability scanning responsibilities.	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Security Monitoring	SR-578	The Contractor must monitor and respond to security alerts, advisories, and directives from external organizations specified by EC, that includes: a) generating internal security alerts, advisories, and directives to address a detected security threat, or as directed by EC; b) informing Operators with security responsibilities about security alerts, advisories, and directives , and c) implementing security directives in accordance with time frames specified by EC. In addition to any sources of intelligence on cyber threats and Incidents that the Contractor monitors in its routine operations, the Contractor must also monitor for cyber threats and incidents published in sources identified by EC (e.g. the Canadian Cyber Incident Response Centre (CCIRC) - http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Security Operations Center	SR-580	The Contractor must provide a EC MAN/WAN Services Security Operations Centre with the infrastructure and resources required for the centralized monitoring and resolution of Security Incidents on a 24 hours per day, 7 days per week and 365 days per year basis. <SR-580> The EC MAN/WAN Services Security Operations Centre must: <SR-580> a) coordinate Security Incident response closely with EC; b) be accessible via a unique and dedicated telephone number answered using the official languages of EC (French, English) as requested by the caller; c) act as a point of contact for communications with EC representatives for Security Incidents; d) not affect operations of EC MAN/WAN Services in case of a SOC failure; e) notify EC within 15 minutes if the EC MAN/WAN Services Security Operations Centre is not available; f) provide a contact name that EC can communicate with as necessary during EC MAN/WAN Services Security Operations Centre outage. The EC MAN/WAN Services Security Operations Centre must work with EC's Information Protection Centre for activities that include: <SR-580> a) integration of Security Incident handling processes; b) Security Incident oversight; c) Security Incident handling and response; and d) auditing. The EC MAN/WAN Services SOC must work with EC's IPC and EC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that includes: <SR-580> a) the ability to dispatch the ITSIRT to the Contractor site; and b) allowing EC to provide on-site guidance and coordination.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Security Incident Management	SR-582	The EC MAN/WAN Services Security Operations Center must use Secure Terminal Equipment (STE) provided by EC as Government Furnished Equipment (GFE) and following EC's COMSEC processes that includes a unique and dedicated STE telephone number, to communicate with EC when requested by EC. <SR-582> The Contractor is responsible for any facility improvements that it requires to store and use the STE in accordance with COMSEC processes at no additional cost to EC. <SR-582>	Examine: secure SDLC artefacts - operational policies and procedures detailing the SOC environment; security incident handling procedures; Interview: Contractor personnel with security incident management role and responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Security Operations	Security Incident Management	SR-583	The EC MAN/WAN Services Security Operations Center must accept emails from EC's authorized representatives to a Contractor-provided mailbox with an auto reply to confirm receipt of the email 24 hours per day, 7 days per week, 365 days per year. The Contractor must encrypt the content of emails when requested by EC, in compliance with SR-20. <SR-583>	Examine: secure SDLC artefacts - operational policies and procedures detailing the SOC environment; security incident handling procedures; Interview: Contractor personnel with security incident management role and responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Security Operations	Security Incident Management	SR-584	The EC MAN/WAN Services Security Operations Centre must acknowledge receipt of any email received from EC's authorized representatives, within 15 minutes of receiving the email, 24 hours per day, 7 days per week, 365 days per year.<SR-584>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Security Incident Management	SR-585	The EC MAN/WAN Services Security Operations Centre must authenticate the identity of the originator of any communication using a process approved by EC <SR-585>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Incident Management	SR-586	The Contractor must automatically provide Incident Ticket information by email, to pre-defined distribution lists specified by EC, for Incidents where EC specifies: <SR-586 > a) the information from the Incident Ticket; and b) criteria for selecting Incidents Tickets (e.g. priority, content of Incident Ticket). The Contractor must continue to automatically send an email update about an Incident Ticket, based on frequency specified by EC for the distribution list, until the Incident Ticket is closed or EC cancels the automatic update reporting for the Incident. <SR-586> Security Incident Tickets must include the following additional information:<SR-586> a) type and description of attack/event; b) whether attack appears to have been successful, and the impact; c) attack scope (e.g. Contractor Core Network; Contractor Access Network; Service Portal, etc); d) estimated number of EC SDAs and/or NAPs affected; e) list of SDPs affected and/or NAPs affected; f) apparent source/origin of attack/Incident/event; g) date/time of attack/Incident/event; h) estimated injury level /sector; i) estimated impact level; j) attack/Incident/event duration; k) actions taken; l) status of mitigations, and m) applicable logs or evidence data. The Contractor must retain Security Incident Tickets for the duration of the Contract. <SR-586>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Incident Management	SR-594	The Contractor must create an Incident Ticket or Security Incident Ticket for each Incident detected by the Contractor and reported by EC, regardless of the cause (e.g. site power), and set the status of the Incident Ticket or Security Incident Ticket to open. <SR-594> The Contractor must not include any classified and potentially harmful information in Security Incident Tickets. <SR-594> The Contractor must separate information that identifies and details Security Incidents from all other types of Incidents. The Contractor must provide Contractor Security Incident Data that has or could impact on delivery of EC MAN/WAN Services to the EC MAN/WAN Services Security Operations Centre. <SR-594> The storage of EC MAN/WAN Services Security Operations Data must be physically dedicated to EC. <SR-594>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Security Incident Management	SR-595	The Contractor must report all suspected or actual privacy and security violations for EC MAN/WAN Services Data and Client Data as Security Incidents.<SR-595>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Incident Management	SR-597	The Contractor must open an Incident Ticket within 5 minutes of detecting an Incident or receiving a notice from EC reporting an Incident. <SR-597>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Incident Management	SR-598	The Contractor must update the Incident Ticket log within 5 minutes of a change in status for any Incidents identified by EC as high priority, and within 15 minutes of a change in status for all other Incidents.<SR-598>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Incident Management	SR-599	The Incident Ticket must include the following dedicated information fields for all Incidents: <SR-599> a) Contractor's Ticket number; b) Incident description; c) Incident originator contact information (name, telephone number and email address); d) Incident originator language; e) related Incident Tickets; f) date and time stamp when Incident Ticket initiated; g) date and time stamp when Incident Ticket closed; h) Incident Ticket type (as specified by EC); i) Incident Ticket impact; j) Incident Ticket priority; k) Incident Ticket status (i.e. open, closed, in progress, suspended, cancelled etc.); l) Incident Ticket escalations; m) EC's ticket number; n) affected SDPs; o) Contractor contact information (name, telephone number and email address); p) EC identifier (If applicable); q) interactions with third parties; r) activity log; s) root cause (if available); t) estimated time for resolution (updated every 15 minutes); u) resolution description and v) outage time; w)adjusted outage time.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Security Incident Management	SR-601	The Contractor must participate in a Security Incident meeting within 1 Business Day of a request by EC, with the following agenda items: <SR-601> a) date/time of Security Incident; b) estimated injury level /sector; c) estimated impact level; d) duration; e) description; f) whether attack appears to have been successful and impact; g) scope (e.g. Contractor Core Network; Contractor Access Network; Service Portal; single or multiple Clients); h) estimated number of SDPs and/or NAPs affected; i) list of SDPs affected; j) actions taken; k) apparent source/origin; l) status of mitigations; and m) references to applicable logs or evidence data.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Security Incident Management	SR-602	The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing Service Portal malicious content) to contain security issues, protect against cyber threats and address vulnerabilities in accordance with EC's priority level assignments for Security Incidents defined in Table 13.< SR-602>	Examine: secure SDLC artefacts - EC MAN/WAN Services design documentation; EC MAN/WAN Services system configuration settings documentation for firewall blocks, customized Intrusion Detection Prevention signatures; Test: ST&E test results demonstrating the security incident information compliant with SR-602.	Completeness, Effectiveness, Reliability	Yes	
Security Operations	Security Incident Management	SR-603	The Contractor must encrypt EC MAN/WAN Services Security Data using cryptographic standards in compliance with SR-20 if the information is stored or transmitted in electronic form. <SR-603>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Security Incident Management	SR-606	The Contractor must provide a Security Incident post- mortem report to EC, within 72 hours of a request by EC, that includes, but is not limited to:<SR-606> a) Security Incident Ticket number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) residual limitations/issues with the EC MAN/WAN Services Infrastructure, and j) recommendations to improve the Security Posture of the EC MAN/WAN Services Infrastructure.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Emergency Measures	SR-612	The Contractor must create an Emergency Service Request for each mitigation measure required to contain a Security Incident, and must implement the Emergency Service Request in accordance with the priority established by EC for the Security Incident. <SR- 612>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Emergency Measures	SR-613	The Contractor must continue to automatically send daily email updates about Service Requests until the Service Request is closed or EC cancels the automatic update reporting for the change. <SR-613>	Examine: secure SDLC artefacts - Access control policy; procedures addressing EC MAN/WAN Services information flow enforcement; procedures addressing source and destination domain identification and authentication, and information transfer error handling; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; other relevant documents or records; Test: ST&E test results that demonstrate the automated mechanisms implementing information flow enforcement policy.	Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Investigations	SR-614	The Contractor must perform audit and investigation activities for the Service Portal that includes: a) identifying authorized and unauthorized access to Service Portal Computing Infrastructure through Operator and Boundary Protection audit logs; and b) forensic analysis of OS system partitions, application partitions and application data stores.	Examine: secure SDLC artefacts - Access control policy; procedures addressing EC MAN/WAN Services information flow enforcement; procedures addressing source and destination domain identification and authentication, and information transfer error handling; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; other relevant documents or records; Test: ST&E test results that demonstrate the automated mechanisms implementing information flow enforcement policy.	Effectiveness, Reliability	No	
Security Operations	Investigations	SR-615	The Contractor must restrict access to EC MAN/WAN Services Data accessible from the Service Portal, specified by EC, within 2 Business Days of a request by EC. The Contractor must permanently delete EC MAN/WAN Services Data specified by EC within 2 Business Days of a request by EC, using a process approved by EC, and must provide EC with evidence within 2 Business Days following deletion of the data that the data was deleted.	Examine: secure SDLC artefacts - EC MAN/WAN Services design documentation for permanent deletion; EC MAN/WAN Services system configuration settings documentation for permanent deletion tools; Test: ST&E test results demonstrating the investigations compliant with SR-615.	Completeness, Effectiveness, Reliability	No	
Security Operations	Investigations	SR-617	The Contractor must provide EC MAN/WAN Services Data specified by EC within 2 Business Days of a request by EC in a COTS file format and media specified by EC.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	
Security Operations	Investigations	SR-618	The Contractor must have forensic procedures and safeguards in place that ensures: a) the maintenance of a chain of custody for the audit information; and b) the collection, retention, and presentation of evidence that can demonstrate the integrity of the evidence.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Security Reports	SR-622	The Contractor must provide a monthly service operations summary report that includes: a) summary of Security Incidents, remedial actions taken and unresolved Security Incidents carried over from the previous report; and b) summary of patches and security patches implemented. <SR-622>	Examine: secure SDLC artefacts - EC MAN/WAN Services system audit and accountability policy; procedures addressing auditable events; security plan; list of EC MAN/WAN Services Service-defined auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; other relevant documents or records. Examine: EC MAN/WAN Services system system and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the EC MAN/WAN Services system; list of recent security flaw remediation actions performed on the EC MAN/WAN Services system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct EC MAN/WAN Services system flaws; other relevant documents or records. Interview: Contractor personnel with auditing and accountability responsibilities and personnel with flaw remediation responsibilities.		Yes	
Security Operations	Security Reports	SR-624	The Contractor must provide a monthly Security Threat Report to EC that includes, by frequency of occurrence, the: <SR-624> a) top 10 threat vectors to EC MAN/WAN Services; b) top 10 targeted protocols/applications; c) top 10 origins/sources of attack; and d) top 10 types of attacks (e.g. injection, phishing, DoS, cross-site scripting, etc.). Upon request by EC and at a frequency not greater than monthly, the Contractor must provide a Security Incident Report to EC, and within 5 Business Days of a request by EC, that includes the following information for Security Incidents specified by EC: <SR-624> a) Security Incident Ticket number; b) Security Incident Ticket opened/closed date; c) threat vector; d) targeted service/protocol/application; e) origin/source of attack; and f) type of attack (e.g. injection, phishing, DoS, cross-site scripting, etc.).	Examine: secure SDLC artefacts - EC MAN/WAN Services System incident response policy; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; other relevant documents or records. Interview: Contractor personnel with incident reporting responsibilities.	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Security Reports	SR-625	The Contractor must provide a weekly Security Breach Report to EC that includes:<SR-625> a) number of Security Incidents; b) number of security investigations completed; c) average and highest response time to Security Incidents; and d) average and highest security investigation completion time.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Infrastructure	Access Control	SR-633	The Service Portal must include User access as follows:<SR-633> i) secure access connection (e.g. TLS 1.2); ii) minimize the requirement for additional account logins to the various services; iii) request a unique User ID and password; iv) enforce a configurable idle session timeout period, as specified by EC; v) deactivate the User account after a password is entered incorrectly after a number of times specified by EC; and vi) end a session (log out) securely (all session cookies, if any, must be deleted).	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Security Reports	SR-634	The Contractor must provide EC with access to EC MAN/WAN Services Security Data via the EC MAN/WAN Services SOC-to-EC IPC connection (see SR-192).	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	
Policy & Procedures	Access Control	SR-128	The Contractor must conduct an annual review of the access control policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Operational Artefacts - Access control policy & procedures, supporting audit/compliance reports; Interview: Contractor personnel with access control responsibilities	Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Access Control	SR-129	The Contractor must manage Operator and Administrator accounts by: a) identifying account types (i.e., individual, group, system, device, application, guest, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the EC MAN/WAN Services Contractor Infrastructure and specifying access privileges; d) requiring appropriate approvals for requests to establish accounts; e) selecting an identifier that uniquely identifies the Operator/Administrator; f) assigning the Operator/Administrator identifier to the intended party; g) establishing, activating, modifying, disabling, and removing accounts; h) specifically authorizing and monitoring the use of guest and temporary accounts; i) notifying the account administrator when temporary accounts are no longer required and when Operators and Administrators are terminated, transferred, or EC MAN/WAN Services Contractor Infrastructure access privileges change; j) preventing reuse of Operator/Administrator identifiers for at least one year; k) deactivating: i) temporary accounts that are no longer required; ii) accounts of terminated or transferred Operators and Administrators; iii) accounts after a number of days of inactivity, as specified by EC, and iv)) temporary and emergency accounts over a given age, as specified by EC; l) granting access to the EC MAN/WAN Services Infrastructure and EC MAN/WAN Services Data in accordance with: i) a valid access authorization; ii) role-based system usage, and iii) need-to-know data access restrictions; m) reviewing Operator/Administrator accounts monthly to identify inactive accounts and accounts with abnormal activity; n) locking the account after five unsuccessful login attempts occurring within 5 minutes; and keeping the account locked until manually unlocked by another account administrator.	Examine: Operational Artefacts - Access control policy, account management procedures, Complete list of accounts including guest/temporary, supporting documentation for account activation, change or removal; Interview: Contractor personnel with account management responsibilities	Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Access Control	SR-133	The Contractor must provide logging of the following Operator and Administrator account events in accordance with the event logging requirements for Level 3 assurance, as detailed in ITSG-31: a) account creation; b) account modifications; c) account disabling; d) account termination; e) successful authentication; and unsuccessful authentication.	Examine: Development/Design Artefacts - Detail Level Design, Configuration/Build Books; Examine: Operational Artefacts - Account management procedures, audit/compliance reports; Examine: Security Test and Evaluation results	Effectiveness, Reliability	No	
Infrastructure	Access Control	SR-134	The Contractor must define a working hours policy and monitor EC MAN/WAN Services Operator and Administrator accounts utilization against that policy, including: a) logging atypical usage of administrator accounts; and b) alerting designated Contractor and EC resources of atypical usage of administrator accounts. The Contractor must provide the atypical utilization log for Operator/Administrator accounts to EC within 1 Business Day of a request by EC. The Contractor must ensure that EC MAN/WAN Services Operators and Administrators are logged out at the end of their working shift.	Examine: Operational Artefacts - Account management procedures, security reports, audit/compliance reports; Examine: Development/Installation Artefacts - Configuration/build books, Detailed Level Design; Interview: Contractor Operational Resources	Compliance, Effectiveness, Completeness	No	
Infrastructure	Access Control	SR-135	The Contractor must manage Operator and Administrator accounts as follows: a) create Operator/Administrator accounts in accordance with role-based access profiles that specify privileges; b) track and monitor Operator/Administrator role assignments; and c) adjust role assignments as Operator/Administrator roles change.	Examine: Operational Artefacts - Account management procedures, RACI for privileged account, audit/compliance reports; Examine: Development/Installation Artefacts - Configuration/build books, Detailed Level Design; Interview: Contractor Operational Resources with account management responsibilities.	Compliance, Effectiveness, Completeness	No	
Infrastructure	Access Control	SR-136	EC MAN/WAN Services Contractor Infrastructure must require access authorizations for all Operators and Administrators, unless otherwise approved by EC.	Examine: Development/Installation Artefacts - Configuration/build books; Examine: Operational Artefacts - Access control policy, access enforcement procedures, audit/compliance reports, approved user privileges authorization records; Test: ST&E results confirming the implemented access control policy is being enforced.	Compliance, Effectiveness, Completeness	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Access Control	SR-139	The Contractor must implement separation of duties for its Operators, as necessary, to prevent malevolent activity without collusion according to the role-based access profile assigned to the Operator.	Examine: Development/Installation Artefacts - Design Documentation, configuration/build books; Examine: Operational Artefacts - Access control policy, access enforcement and separation of duties procedures, list of approved privileged commands and approved user privileges authorization; Interview: Contractor resources with access enforcement responsibilities; Test: ST&E results related to separation of duties or dual authorization mechanisms.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Access Control	SR-140	The Contractor must implement a "least privileges" policy for its Operators as follows: a) access control mechanisms must be configured to implement least privilege, allowing only authorized access for Operators (and processes acting on their behalf) that are necessary to accomplish assigned tasks; b) create non-privileged accounts to be used for non- operations tasks; c) restrict authorization of super user accounts (e.g., root) to a highly-controlled number of Operators; d) restrict sharing of Operator accounts; and e) uniquely identify the human Operator who has performed each operation on the EC MAN/WAN Services Contractor Infrastructure.	Examine: Development/Installation Artefacts - Design Documentation, configuration/build books; Examine: Operational Artefacts - Access control, least privileges and documented details of users & resources requiring enforcement of least privileges policies, access enforcement procedures; Interview: Contractor resources with access enforcement responsibilities Test: ST&E result confirming the implementation and operation of least privileges policy.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Access Control	SR-145	The EC MAN/WAN Services Contractor Infrastructure, that is accessible using Internet Protocol, must include access control mechanisms that: a) prevent access without identification, authentication, and authorization; b) display a EC-approved logon warning banner that authorized Operators and Administrators must acknowledge prior to being granted access to EC MAN/WAN Services Infrastructure components; and c) notifies the Operators and Administrators, upon successful logon (access), of the date and time of the last logon (access). The access control mechanisms for EC MAN/WAN Services Infrastructure, that is accessible using Internet Protocol, must include an Operator and Administrator session lock mechanism that: a) prevents further access to infrastructure components by automatically initiating a session lock after a period of inactivity for a configurable time period to be specified by EC; b) prevents further access to infrastructure components by initiating a session lock when requested by the Operator/Administrator; c) displays a screen saver that contains no meaningful information to completely replace what was previously displayed on the screen upon activation of a session lock; and d) unlocks the session after successful authentication of the Operator/Administrator.	Examine: Development/Installation Artefacts - Design Documentation; Examine: Operational Artefacts - Access control policy, configuration settings and procedures related to logon notification; audit results; Test: ST&E Artefacts covering the requirements related test results.	Effectiveness, Reliability	No	
Infrastructure	Access Control	SR-146	Unless requested by EC, the Contractor must disable any TCP/UDP listening ports on EC MAN/WAN Services Infrastructure. Access control methods in compliance with SR-145 and SR-235 must be in place for all ports that are open for network management purposes.	Examine: Development/Installation Artefacts - Design Documentation; Examine: Operational Artefacts - Access control policy, configuration settings and associated documentation; audit results; Interview: Contractor personnel with responsibilities for network design and network management. Test: ST&E Artefacts covering the requirements related test results.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Access Control	SR-158	Any use of IP/Layer 3 Remote Management within the EC MAN/WAN Services must take place using a method approved by EC that must include: a) restricting the Remote Management of EC MAN/WAN Services Contractor Infrastructure to dedicated Operator Consoles located in Network Security Zones in compliance with SR-100 to SR-106; b) documenting allowed methods of Remote Management with usage restrictions and implementation guidance included in the SA&A Gate 1 and Gate 2 deliverables; c) monitoring for unauthorized Remote Management; d) authorizing Remote Management prior to connection; e) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods; f) routing Remote Management of EC MAN/WAN Services Contractor Infrastructure components through a limited number of managed access control points; and g)protecting information about Remote Management mechanisms from unauthorized use and disclosure.	Examine: secure SDLC artefacts – EC MAN/WAN Services system access control policy; procedures addressing remote access to the EC MAN/WAN Services system; EC MAN/WAN Services system configuration settings and associated documentation; information system audit records; other relevant documents or records; Interview: Contractor personnel with remote access authorization, monitoring, and control responsibilities, with responsibilities for monitoring remote connections to the information system. Test: ST&E test results that demonstrate remote access methods for the information system as per SR-158.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Access Control	SR-160	The Contractor must implement/manage Non-local Access by: a) using two-factor authentication in compliance with SR- 292 at the EC MAN/WAN Services Security Operations Zone and EC MAN/WAN Services Network Operations Zone boundary; b) using session encryption in compliance with SR-20, and SR-420 where split-tunnelling must be disabled; and c) ensuring compliance with all other terms and conditions of the EC MAN/WAN Services Contract.	Examine: Development/Installation Artefacts - Design documentation, configuration settings; Examine: Operational Artefacts - Access control policy, procedures addressing wireless implementation disabling, audit reports of systems; Test: ST&E results demonstrating the disabling of all wireless capabilities with EC MAN/WAN Services Service Infrastructure.	Compliance, Completeness, Effectiveness, Reliability	No	
Infrastructure	Access Control	SR-168	The Contractor must not allow wireless access for management of the EC MAN/WAN Services Infrastructure, unless otherwise approved by EC,with the exception of wireless access deployed within its internal corporate network for Non-local Access that is in compliance with SR-160.	Examine: Development/Installation Artefacts - Design documentation, configuration settings; Examine: Operational Artefacts - Access control policy, procedures addressing wireless implementation disabling, audit reports of systems; Test: ST&E results demonstrating the disabling of all wireless capabilities with EC MAN/WAN Services Service Infrastructure.	Compliance, Completeness, Effectiveness, Reliability	No	
Infrastructure	Access Control	SR-170	For the EC MAN/WAN Services Security Operations Zone and the EC MAN/WAN Services Network Operations Zone, the Contractor must: a) continuously monitor for the presence of wireless access points connected to the zone network; b) immediately disable any wireless access point if one is discovered ; and c) open a Security Incident Ticket if a wireless access point is discovered.	Examine: Operational Artefacts - Access control policy, procedures addressing wireless implementation disabling, audit reports of systems; Interview: Contractor resources responsible for monitoring wireless connections to EC MAN/WAN Services Service Infrastructure; Test: ST&E results demonstrating the disabling of all wireless capabilities with EC MAN/WAN Services Service Infrastructure.	Effectiveness; Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Access Control	SR-171	The Contractor must permanently disable all wireless networking functions embedded within Computing Infrastructure and Internetwork Components located in the EC MAN/WAN Services Security Operations Zone and the EC MAN/WAN Services Network Operations Zone.	Examine: Operational Artefacts - Access control policy, procedures addressing wireless implementation disabling, audit reports of systems; Interview: Contractor resources responsible for monitoring wireless connections to EC MAN/WAN Services Service Infrastructure; Test: ST&E results demonstrating the disabling of all wireless capabilities with EC MAN/WAN Services Service Infrastructure.	Effectiveness; Reliability	No	
Infrastructure	Access Control	SR-173	The Contractor must not allow the use of Mobile Devices to access the EC MAN/WAN Services Infrastructure. The Contractor must not allow the use of mobile broadband modems on the EC MAN/WAN Services Infrastructure, unless otherwise approved by EC.	Examine: Operational Artefacts - Access control policy, procedures addressing use of portable/mobile devices implementation disabling, audit reports of systems; Examine: Development/Installation Artefacts - Detailed Design documents; Interview: Contractor resources responsible for monitoring mobile devices use within EC MAN/WAN Services Service Infrastructure; Test: ST&E results demonstrating the disabling of access to all mobile devices with EC MAN/WAN Services Service Infrastructure.	Effectiveness; Reliability	No	
Infrastructure	Access Control	SR-178	The Contractor must obtain EC's approval for the use of external (i.e., non-Contractor) information systems and telecommunications services associated with the delivery of EC MAN/WAN Services.	Examine: Operational Artefacts - Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; Interview: Contractor personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems.	Effectiveness; Reliability	No	
Infrastructure	Access Control	SR-180	The Contractor must control and limit the use of Contractor-controlled Portable Digital Media (e.g., thumb drive) as follows: a) restrict the use to authorized Operators only; b) once used on EC MAN/WAN Services Infrastructure, restrict the use to those EC MAN/WAN Services Infrastructure components only; and c) perform malicious code scans prior to any use on EC MAN/WAN Services Contractor Infrastructure.	Examine: Operational Artefacts - Access control policy; procedures addressing the use of portable storage media; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system connection or processing agreements; account management documents.	Effectiveness; Reliability	No	
Infrastructure	Access Control	SR-183	The Contractor must obtain EC's approval before making any EC MAN/WAN Services Data publicly available.	Examine: Operational Artefacts - Access control policy; procedures addressing the use of portable storage media; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system connection or processing agreements; account management documents.	Effectiveness; Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Policy & Procedures	Awareness & Training	SR-184	The Contractor must conduct an annual review of the security awareness and training policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Operational Artefacts - Security awareness and training policy and procedures; other relevant documents or records; Interview: Contractor personnel with security awareness and training responsibilities.	Completeness, Effectiveness	No	
Infrastructure	Awareness & Training	SR-186	The Contractor must provide security awareness and training for Operators as follows: a) as part of initial training for new Operators; b) before authorizing Operators with access to the EC MAN/WAN Services Infrastructure or performing assigned duties; and c) annually, or when security-impacting changes to the EC MAN/WAN Service occur.	Examine: Development/Installation Artefacts - Design Documentation, configuration details; Examine: Operational Artefacts - Access control and remote access policy, procedures for remote access, audit reports of monitoring related to remote access; Test: ST&E test results related to remote access controls and monitoring.	Completeness, Reliability	No	
Infrastructure	Awareness & Training	SR-187	The Contractor must document the security awareness training for Operators, including who received what training course and when, and retain the records for the last 3 years.	Examine: Operational Artefacts - Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of GC policies; security awareness training curriculum; security awareness training materials; training records; Interview: Contractor personnel comprising the EC MAN/WAN Services system administrator/operator user community.	Completeness, Effectiveness	No	
Policy & Procedures	Logging and Auditing	SR-188	The Contractor must conduct an annual review of the audit and accountability policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Development/Installation Artefacts - Design Documentation, configuration details; Examine: Operational Artefacts - Access control and remote access policy, procedures for remote access, audit reports of monitoring related to remote access; Test: ST&E test results related to remote access controls and monitoring.	Completeness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Logging and Auditing	SR-193	The Contractor must log the following events for the Contractor Security Operations Zone, Contractor OAM Zone, Contractor Core Network and Contractor Access Network (excluding Contractor Equipment) and store the log data on the Contractor SIEM: a) use of privileged operator accounts; b) accepted operator login and logout, with date/time stamps; c) rejected login attempts, with date/time stamps; d) accepted operator/User login and logout, with date/time stamps, to EC MAN/WAN Services OAM Data and EC MAN/WAN Services System Data; e) rejected operator/User login attempts, with date/time stamps, to EC MAN/WAN Services OAM Data and EC MAN/WAN Services System Data; f) grant, modify, or revoke access rights, including adding a new operator/User or group, changing operator/User privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and operator/User password changes; g) configuration changes, including installation of software patches and updates, or other installed software changes; h) process start-up, shutdown, or restart; i) process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and j) detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Logging and Auditing	SR-194	The Contractor must log the following events for the EC MAN/WAN Services Security Operations Zone, EC MAN/WAN Services Network Operations Zone and Contractor Equipment and store the log data on the EC SIEM: a) use of privileged Operator accounts; b) accepted Operator login and logout, with date/time stamps; c) rejected login attempts, with date/time stamps; d) accepted Operator/User login and logout, with date/time stamps, to EC MAN/WAN Services Security Data and EC MAN/WAN Services SDP Device Configuration Data; e) rejected Operator/User login attempts, with date/time stamps, to EC MAN/WAN Services Security Data and EC MAN/WAN Services SDP Device Configuration Data; f) grant, modify, or revoke access rights, including adding a new Operator/User or group, changing Operator/User privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and Operator/User password changes; g) configuration changes, including installation of software patches and updates, or other installed software changes; h) process start-up, shutdown, or restart; i) process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and j) detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	
Security Operations	Logging and Auditing	SR-195	The Contractor must review and update the list of auditable events for EC MAN/WAN Services and the EC MAN/WAN Services Contractor Infrastructure on an annual basis and provide the updated list to EC within 20 Business Days of the Contract anniversary date.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Logging and Auditing	SR-197	The Contractor must log visitor entry requests (accepted and rejected) to a Contractor EC MAN/WAN Services Facility. The Contractor must provide EC with a copy of the visitor entry request log to a Contractor EC MAN/WAN Services Facility within 5 Business Days of a request from EC.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of organization-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	
Security Operations	Logging and Auditing	SR-198	The Contractor must manage the capacity of the audit record storage by: a) allocating enough audit record storage capacity to maintain audit log data for a minimum of two years; b) configuring auditing to prevent storage capacity being exceeded; c) alerting the EC MAN/WAN Services Security Operations Center when the allocated audit record storage volume reaches 75% of the audit record storage capacity; and d) adding audit record storage capacity when the allocated audit record storage volume reaches 75% of the audit record storage capacity.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing audit storage capacity; EC MAN/WAN Services system audit records; Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; EC MAN/WAN Services-defined audit record storage capacity for EC MAN/WAN Services system components that store audit records; list of EC MAN/WAN Services-defined auditable events; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records Test: ST&E results related to audit record storage capacity and related configuration settings.	Compliance, Completeness, Effectiveness, Reliability	No	
Security Operations	Logging and Auditing	SR-199	The Contractor must respond to auditing failures of the EC MAN/WAN Services Infrastructure by: a) alerting the EC MAN/WAN Services Security Operations Centre; and b) initiating a Security Incident Ticket.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing response to audit processing failures; list of ESP/SSC personnel to be notified in case of an audit processing failure; EC MAN/WAN Services system audit records; Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; Test: ST&E results covering the mechanisms implementing information system response to audit processing failures.	Compliance, Completeness, Effectiveness, Reliability	No	
Security Operations	Logging and Auditing	SR-208	The EC MAN/WAN Services Contractor Infrastructure must use internal system clocks that are synchronized with an authoritative time source approved by EC, to generate time stamps for audit records.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing time stamp generation; EC MAN/WAN Services system audit records; Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; Test: ST&E test results associated with mechanisms implementing time stamp generation.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Logging and Auditing	SR-210	The Contractor must protect audit information from unauthorized access, modification, and deletion. The Contractor must implement technology in the Contractor SIEM and EC SIEM that incorporates tamper resistant cryptographic mechanisms in compliance with SR-20 to protect the integrity of audit information. The Contractor must backup audit records onto a different system or medium than the system being audited, in accordance with the Service Continuity Plan.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records]. Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation, system or media storing backups of EC MAN/WAN Services system audit ecords; EC MAN/WAN Services system audit records; EC MAN/WAN Services system hardware settings; Interview: Contractor personnel with auditing and accountability responsibilities. Test: ST&E test results associated with EC MAN/WAN Services mechanisms implementing audit information protection.	Completeness, Effectiveness, Reliability	No	
Security Operations	Logging and Auditing	SR-212	The Contractor must authorize access to audit functionality to a limited subset of Operators with privileged accounts. The Contractor must implement separation of duties for the EC MAN/WAN Services Contractor Infrastructure management and audit roles by ensuring the same individual is not involved in both roles	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures, EC MAN/WAN Services system audit records; Examine: Development/Installation Artefacts - EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; Interview: Contractor personnel with auditing and accountability responsibilities.	Completeness, Effectiveness, Reliability	No	
Policy & Procedures	Configuration Management	SR-217	The Contractor must conduct an annual review of the configuration management policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Development/Installation/Integration/Operational Artefacts - Configuration management policy and procedures; other relevant documents or records; Interview: Contractor personnel with configuration management and control responsibilities.	Completeness, Effectiveness, Reliability	No	
Configuration Management	Configuration Management	SR-218	The Contractor must develop, document, and maintain the current baseline configuration of the EC MAN/WAN Services Infrastructure with traceability back to previous versions. <SR-218>	Examine: secure SDLC phases - Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the EC MAN/WAN Services system; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system architecture and configuration documentation; other relevant documents or records; Interview: Contractor personnel with configuration change control responsibilities; Test: ST&E test result related to demonstrate mechanisms implementing baseline configuration maintenance.	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Configuration Management	Configuration Management	SR-221	The Contractor must only allow authorized software, as documented by the Contractor, to be installed and run on the EC MAN/WAN Services Contractor Infrastructure.	Examine: secure SDLC - Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the EC MAN/WAN Services system; list of software programs not authorized to execute on the EC MAN/WAN Services system; EC MAN/WAN Services system architecture and configuration documentation; security plan; other relevant documents or records;	Completeness, Effectiveness, Reliability	No	
Configuration Management	Configuration Management	SR-223	The Configuration Management performed by the Contractor for the EC MAN/WAN Services must include processes for:<SR-223> a) determining the types of changes that are configuration controlled; b) approving configuration-controlled changes with explicit consideration for security impact analyses; c) documenting approved configuration-controlled changes; d) retaining and reviewing records of configuration- controlled changes; and e) auditing activities associated with configuration- controlled changes. The Contractor must ensure that only authorized Configuration Items are released and implemented in EC MAN/WAN Services Infrastructure.<SR-223>	Examine: secure SDLC artefacts - EC MAN/WAN Services configuration management policy; configuration management plan; procedures addressing EC MAN/WAN Services system configuration change control; EC MAN/WAN Services system architecture and configuration documentation; security plan; change control records; EC MAN/WAN Services system audit records; other relevant documents or records. Interview: Contractor personnel with configuration change control responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Configuration Management	Configuration Management	SR-233	The Contractor must review Operator privileges annually.	Examine: secure SDLC - Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the EC MAN/WAN Services system; security impact analysis documentation; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system architecture and configuration documentation; change control records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system test and operational environments; other relevant documents or records; Interview: Contractor personnel with responsibilities for determining security impacts prior to implementation of information system changes.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Configuration Management	Configuration Management	SR-235	The Contractor must manage the configuration settings for EC MAN/WAN Services Infrastructure by:<SR-235> a) specifying component configuration settings to implement Operator least privilege/functionality; b) documenting exceptions to configuration settings; and c) monitoring and controlling changes to the configuration settings in accordance with Request Fulfillment and Configuration Management processes. The Contractor must ensure that any EC MAN/WAN Services SDP Device Configuration Data held is encrypted on data storage systems in compliance with SR-20. <SR- 235>	Examine: secure SDLC - Configuration management policy; configuration management plan; procedures addressing configuration settings for the EC MAN/WAN Services system; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; security configuration checklists; other relevant documents or records; Interview: Contractor personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities; Test: ST&E test results related to the demonstration of mechanisms implementing the centralized management, application, and verification of configuration settings.	Completeness, Effectiveness, Reliability	Yes	
Configuration Management	Configuration Management	SR-237	The Contractor must use an automated mechanism to centrally manage, apply, and verify a EC MAN/WAN Services Internetwork Operational Configuration that exists at an SDP. <SR-237>	Examine: secure SDLC - Configuration management policy; configuration management plan; procedures addressing least functionality in the EC MAN/WAN Services system; security plan; EC MAN/WAN Services system configuration settings and associated documentation; security configuration checklists; other relevant documents or records; Interview: Contractor personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the EC MAN/WAN Services system; Test: ST&E test results associated with the demonstration of EC MAN/WAN Services system disabling or restricting functions, ports, protocols, and services as well as mechanisms preventing software program execution on the EC MAN/WAN Services system.	Completeness, Effectiveness, Reliability	Yes	
Configuration Management	Configuration Management	SR-244	The Contractor must develop, document, and maintain an inventory of the EC MAN/WAN Services Infrastructure components that:<SR-244> a) accurately reflects their current configuration; b) is at the level of granularity for tracking and reporting as specified in the Contractor's configuration management plan that has been approved by EC; c) is available for review and audit by EC, and d) is updated as an integral part of component installations, removals, and EC MAN/WAN Services Request Fulfillment.	Examine: secure SDLC - Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records; Interview: Contractor personnel with information system installation and inventory responsibilities; Test: ST&E test results demonstrating the automated mechanisms implementing EC MAN/WAN Services system component inventory management	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Configuration Management	Configuration Management	SR-246	The Contractor must maintain an inventory of the components used as Contractor Equipment at each SDP, and create a Security Incident Ticket for addition of unauthorized components. <SR-246> The Contractor must use automated mechanisms to maintain an inventory of the components used and create a Security Incident Ticket for addition of unauthorized components for: <SR-246> a) the EC MAN/WAN Services Security Operations Zone; and b) the EC MAN/WAN Services Network Operations Zone.	Examine: secure SDLC - Configuration management policy; configuration management plan; procedures addressing EC MAN/WAN Services system component inventory; security plan; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system inventory records; component installation records; change control records; other relevant documents or records; Interview: Contractor personnel with information system installation and inventory responsibilities; Test: ST&E test results that demonstrate the automated mechanisms for detecting unauthorized components/devices on the EC MAN/WAN Services system as well as an automated mechanisms implementing EC MAN/WAN Services system component inventory management.	Completeness, Effectiveness, Reliability	Yes	
Service Continuity	Contingency Planning	SR-252	The Contractor must conduct an annual review of the service continuity and contingency planning policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Contingency planning policy; procedures addressing contingency operations for the EC MAN/WAN Services system; contingency plan; security plan; business impact assessment; other relevant documents or records; Interview: Contractor personnel with contingency planning and plan implementation responsibilities; Contractor personnel with incident handling responsibilities.	Completeness, Effectiveness, Reliability	No	
Service Continuity	Contingency Planning	SR-254	The Contractor must perform capacity planning so that necessary capacity for processing, telecommunications, and environmental support exists during contingency operations.<SR-254> The Contractor must train its personnel annually in their contingency roles and responsibilities for EC MAN/WAN Services which includes simulated events to facilitate effective response in crisis situations. <SR-254>	Examine: Operational Artifacts -Contingency planning policy; procedures addressing contingency operations for the EC MAN/WAN Services system; contingency plan; capacity planning documents; other relevant documents or records; Interview: Contractor personnel with contingency planning and plan implementation responsibilities.	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Service Continuity	Contingency Planning	SR-262	The Contractor must test the Service Continuity Plan (all processes, procedures, roles, responsibilities etc) on an annual basis, and provide the test results to EC within 10 Business Days of completion of the testing. Test failures must be reported to EC as a Security Incident. <SR-262> The Contractor must correct any problems identified during the testing of the Service Continuity Plan within 60 Business Days after completion of the testing. <SR-262> The Contractor must provide to EC within 40 Business Days of a request, evidence not greater than 12 months old, (e.g. test results, evaluations, and audits, etc.) that the Service Continuity Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting the service continuity requirements for EC MAN/WAN Services. <SR-262> If the Contractor determines that it will take more than 40 Business Days to provide the requested evidence for the Service Continuity Plan, the Contractor must notify EC within 5 Business Days of the original request for evidence, and request an extension in writing, with appropriate justification. Granting an extension is within EC's sole discretion. <SR-262>	Examine: Operational Artefacts - Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; automated mechanisms supporting contingency plan testing/exercises; contingency plan testing and/or exercise documentation; other relevant documents or records; Interview: Contractor personnel with responsibilities for reviewing or responding to contingency plan tests/exercises, contingency planning, plan implementation, EC MAN/WAN Services system recovery and reconstitution responsibilities, and testing responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Service Continuity	Contingency Planning	SR-268	The Contractor must identify potential accessibility problems to the secondary storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions in the Service Continuity Plan.<SR-268>	Examine: Operational Artefacts - contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records;	Completeness, Effectiveness, Reliability	Yes	
Service Continuity	Contingency Planning	SR-269	The Contractor must work in conjunction with EC to establish national restoration priorities for EC MAN/WAN Services in an order of precedence as specified by EC.<SR-269>	Examine: Contingency planning policy; procedures addressing contingency operations for the EC MAN/WAN Services system; contingency plan; security plan; business impact assessment; other relevant documents or records; Interview: Contractor personnel with contingency planning and plan implementation responsibilities; Contractor personnel with incident handling responsibilities.	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Service Continuity	Contingency Planning	SR-280	The Contractor must test the backup data for the EC MAN/WAN Services monthly to verify media reliability and data integrity.<SR-280> The Contractor must use a sample of backup data for EC MAN/WAN Services in the restoration of EC MAN/WAN Services functions as part of service continuity plan testing. The restoration exercise must not be performed using the EC MAN/WAN Services unless otherwise approved by EC. <SR-280>	Examine: Development/Installation Artefacts - Data Center Physical Security Certificates; Backup design documentation; Examine: Operational Artefacts - Contingency planning policy; contingency plan; procedures addressing EC MAN/WAN Services system backup; security plan; EC MAN/WAN Services system backup test results; backup storage location(s); Backup schedules/logs and procedures, audit/compliance reports, contingency plan testing and/or exercise documentation; contingency plan test results; Interview: Contractor personnel with backup responsibilities; Test: ST&E test results demonstrating the backup operations as designed and required.	Completeness, Effectiveness, Reliability	Yes	
Service Continuity	Contingency Planning	SR-283	The Contractor must transfer any backup EC MAN/WAN Services Data, within 24 hours of the backup being done, to an alternate secure storage site.<SR-283>	Examine: Operational Artefacts - Contingency planning policy; contingency plan; procedures addressing EC MAN/WAN Services system backup; backup storage location(s); other relevant documents or records; Interview: Contractor personnel with contingency planning and plan implementation responsibilities; Contractor personnel with EC MAN/WAN Services system backup responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Service Continuity	Contingency Planning	SR-286	The Contractor must refresh the software configuration of EC MAN/WAN Services Infrastructure from configuration- controlled and integrity-protected disk images.<SR-286>	Examine: Operational Artefacts - Contingency planning policy; contingency plan; procedures addressing EC MAN/WAN Services system recovery and reconstitution; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records; Interview: Contractor personnel with EC MAN/WAN Services system recovery and reconstitution responsibilities.	Completeness, Effectiveness, Reliability	Yes	
Policy & Procedures	Identification & Authentication	SR-288	The Contractor must conduct an annual review of the identification and authentication policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Development/Installation/Operational Artefacts - Identification and authentication policy and procedures; other relevant documents or records. Interview: Contractor personnel with identification and authentication responsibilities.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Identification & Authentication	SR-289	The EC MAN/WAN Services Contractor Infrastructure, that is accessible using Internet Protocol, must uniquely identify and authenticate Operators (or processes acting on behalf of Operators). The Contractor must provide distinct accounts to each Operator.	Examine: Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing operator identification and authentication; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system accounts; other relevant documents or records. Test: ST&E test results to demonstrate the automated mechanisms implementing identification and authentication capability for the EC MAN/WAN Services system.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Identification & Authentication	SR-292	For Operator accounts established to perform IP/Layer 3 Remote Management, the Contractor must provide Level 3 Operator authentication for EC MAN/WAN Services Infrastructure in compliance with CSEC ITSG-31, including: a) using two-factor authentication with hardware crypto or one-time password tokens; and b) threat mitigation design against: i) On-line password guessing; ii) Replay; iii) Eavesdropping; iv) Session hijacking; v) Verifier impersonation/phishing; and vi) Man-in-the-middle.	Examine: Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing operator identification and authentication; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; list of privileged EC MAN/WAN Services system accounts; other relevant documents or records. Test: ST&E test results to demonstrate automated mechanisms implementing identification and authentication capability for the information system.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Identification & Authentication	SR-298	The Contractor's designated registration authority must provide EC MAN/WAN Services Infrastructure Operator identifiers and authenticators (e.g. hard crypto token, etc.) in person to the authorized Operator.	Examine: secure SDLC artefacts - EC MAN/WAN Services identification and authentication policy; password policy; procedures addressing authenticator management; security plan; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Test: ST&E test results demonstrating EC MAN/WAN Services automated mechanisms implementing authenticator management functions.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Identification & Authentication	SR-299	The Contractor must require physical identification be presented by an Operator to the Contractor registration authority before the Operator receives identifiers and authenticators to access the EC MAN/WAN Services Infrastructure.	Examine: Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing user identification and authentication; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; list of non-privileged EC MAN/WAN Services system accounts; other relevant documents or records. Test: ST&E test results to demonstrate automated mechanisms implementing identification and authentication capability for the EC MAN/WAN Services system.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Identification & Authentication	SR-301	The Contractor must manage user authentication tokens for Operators and Administrators by: a) verifying, as part of the initial authentication token distribution, the identity of the individual receiving the token; b) establishing initial content for authentication tokens used by the Contractor; c) ensuring that authentication tokens have sufficient strength of mechanism for their intended use; d) establishing and implementing administrative procedures for initial token distribution, lost/compromised or damaged tokens, and the revocation of tokens; e) changing default password tokens upon EC MAN/WAN Services Contractor Infrastructure installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authentication tokens; g) changing/refreshing password tokens at a frequency not exceeding 90 days; h) protecting authentication token content from unauthorized disclosure and modification, and i) requiring Operators and Administrators to take specific measures to safeguard authentication tokens.	Examine: Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing authenticator management; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; list of EC MAN/WAN Services system accounts; other relevant documents or records. Interview: Contractor personnel with responsibilities for determining initial authenticator content. Test: ST&E test results to demonstrate automated mechanisms implementing authenticator management functions.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Identification & Authentication	SR-303	The Contractor must manage IP/Layer 3 device authenticators for EC MAN/WAN Services by: a) verifying, as part of the initial authenticator distribution, the identity of the device receiving the authenticator; b) establishing initial authenticator content for authenticators defined by the Contractor; c) ensuring that authenticators have sufficient strength of mechanism for their intended use; d) establishing and implementing administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators; e) changing default content of authenticators upon EC MAN/WAN Services Infrastructure installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) changing/refreshing static (password-based) authenticators at a frequency not exceeding 90 days; h) protecting authenticator content from unauthorized disclosure and modification, and i) having devices implement specific measures to safeguard authenticators.	Examine: Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing authenticator management; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; list of EC MAN/WAN Services system accounts; other relevant documents or records. Interview: Contractor personnel with responsibilities for determining initial authenticator content. Test: ST&E test results to demonstrate automated mechanisms implementing authenticator management functions.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	Identification & Authentication	SR-305	The EC MAN/WAN Services Contractor Infrastructure must not transmit clear text passwords over any network, with the exception of secure token one-time passwords as approved by EC for two-factor authentication.	Examine: Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing authenticator management; security categorization documentation for the EC MAN/WAN Services system; security assessments of authenticator protections; risk assessment results; security plan; information classification or sensitivity documentation; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Interview: Contractor personnel with responsibilities for authentication management responsibilities; Contractor personnel implementing and/or maintaining authenticator protections. Test: ST&E test results to demonstrate automated mechanisms implementing authenticator management functions.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Identification & Authentication	SR-309	The EC MAN/WAN Services Contractor Infrastructure, that is accessible using Internet Protocol, must obscure feedback of Operator authentication data (e.g., masking password fields) during the authentication process.	Examine: Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing authenticator feedback; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Test: ST&E test results demonstrating the automated mechanisms implementing authenticator feedback.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Identification & Authentication	SR-311	The Contractor must implement a process for authorization of maintenance personnel with physical access to EC MAN/WAN Service Infrastructure that includes: a) maintaining a current list of authorized personnel; and b) ensuring that personnel performing the maintenance on the EC MAN/WAN Service Infrastructure have the required access authorizations..	Examine: secure SDLC artefacts - EC MAN/WAN Services system maintenance policy; procedures addressing controlled maintenance for the EC MAN/WAN Services system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records. Interview: Contractor personnel with EC MAN/WAN Services system maintenance responsibilities.	Completeness, Effectiveness, Reliability	No	
Policy & Procedures	Incident Response	SR-312	The Contractor must conduct an annual review of the Incident response policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Security Operations	Security Incident Management	SR-315	The Contractor must annually test the Security Incident Response Plan that includes: a) documenting the test results; and b) reviewing the test results with EC within 10 Business Days of completing the testing. The Contractor must update the Security Incident Response Plan within 20 Business Days of completing the annual testing.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	No	
Security Operations	Security Incident Management	SR-316	The Contractor must review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing/exercises.<SR-316>	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	
Security Operations	Security Incident Management	SR-324	The Security Incident Response Plan must include: a) how the Contractor plans to identify, report, and escalate Security Incidents; b) a roadmap for implementing the Security Incident response capability that includes preparation, detection, analysis, containment and recovery; c) a description of the structure and organization of the Contractor's Security Incident response capability; d) a high-level approach for how the Security Incident response capability fits into the Contractor's organization, and with its EC MAN/WAN Services third-party suppliers; e) a definition of reportable Security Incidents; f) a definition of metrics for measuring the Contractor's Security Incident response capability; and g)a definition of resources and management support needed to effectively maintain and mature the Security Incident response capability.	Examine: Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; list of EC MAN/WAN Services system auditable events; auditable events review and update records; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; Examine: Development/Installation Artefacts - list of EC MAN/WAN Services-defined auditable events; Interview: Contractor personnel with auditing and accountability responsibilities; Test: EC MAN/WAN Services mechanisms implementing information system auditing of EC MAN/WAN Services-defined auditable events.	Compliance, Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Policy & Procedures	Maintenance	SR-326	The Contractor must conduct an annual review of the maintenance policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: secure SDLC artefacts - EC MAN/WAN Services system maintenance policy and procedures; other relevant documents or records. Interview: Contractor personnel with information system maintenance responsibilities.	Completeness, Effectiveness, Reliability	No	
Maintenance	Maintenance	SR-327	The Contractor must perform the maintenance activities for EC MAN/WAN Services Infrastructure by: a) scheduling, performing, documenting, and reviewing records of maintenance and repairs in accordance with manufacturer or vendor specifications; b) controlling all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location; c) requiring that an official designated by the Contractor explicitly approves the removal of components for off-site maintenance or repairs; d) sanitizing equipment to remove all data from associated media prior to removal from the Contractor's or EC's facilities for off-site maintenance or repairs, and e) checking all potentially impacted security requirements to verify that the controls are still functioning properly following maintenance or repair actions.	Examine: secure SDLC artefacts - EC MAN/WAN Services system maintenance policy; procedures addressing controlled maintenance for the EC MAN/WAN Services system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records. Interview: Contractor personnel with EC MAN/WAN Services system maintenance responsibilities.	Completeness, Effectiveness, Reliability	No	
Maintenance	Maintenance	SR-330	The Contractor must check all media containing diagnostic and test programs for malicious code before the media are used on the EC MAN/WAN Services Infrastructure.	Examine: secure SDLC artefacts - EC MAN/WAN Services system maintenance policy; information system maintenance tools and associated documentation; procedures addressing EC MAN/WAN Services system maintenance tools; EC MAN/WAN Services system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records. Interview: Contractor personnel with EC MAN/WAN Services system maintenance responsibilities. Test: ST&E test results demonstrating automated mechanisms supporting EC MAN/WAN Services system maintenance activities.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Maintenance	Maintenance	SR-331	Maintenance and diagnostic activities performed by the Contractor on the EC MAN/WAN Services Infrastructure must: a) only be performed using maintenance and diagnostic tools approved by the Contractor per SR-329; b) employ Operator identification and authentication techniques in the establishment of maintenance and diagnostic sessions; c) separate the maintenance session from other network sessions by either: i) physically separated communications paths; or ii) logically separated communications paths using cryptographic modules and algorithms in compliance with SR-20; d) record maintenance and diagnostic session Operator activity; e) include a quarterly audit review of the maintenance and diagnostic session records; and f) include initiation of a Security Incident Ticket for any audit anomalies.	Examine: secure SDLC artefacts - EC MAN/WAN Services system maintenance policy; information system maintenance tools and associated documentation; procedures addressing EC MAN/WAN Services system maintenance tools; EC MAN/WAN Services system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records. Interview: Contractor personnel with EC MAN/WAN Services system maintenance responsibilities. Test: ST&E test results demonstrating automated mechanisms supporting EC MAN/WAN Services system maintenance activities.	Completeness, Effectiveness, Reliability	No	
Media Protection	Media Protection	SR-341	The Contractor must restrict access to any media (digital and non-digital) containing EC MAN/WAN Services Data to authorized personnel.	Examine: secure SDLC artefacts - EC MAN/WAN Services system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records. Interview: Contractor personnel with EC MAN/WAN Services system media protection responsibilities.	Completeness, Effectiveness, Reliability	No	
Media Protection	Media Protection	SR-344	The Contractor must mark media containing EC MAN/WAN Services Data with the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	Examine: secure SDLC artefacts - EC MAN/WAN Services system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and EC MAN/WAN Services system output; other relevant documents or records]. Interview: Contractor personnel with EC MAN/WAN Services system media protection and marking responsibilities.	Completeness, Effectiveness, Reliability	No	
Media Protection	Media Protection	SR-345	The Contractor must physically control and securely store media containing EC MAN/WAN Services Data and media containing EC MAN/WAN Services Data awaiting destruction (either on- or off-site) in accordance with the Security Detailed Service Design approved by EC.	Examine: secure SDLC artefacts - EC MAN/WAN Services system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; EC MAN/WAN Services system media; other relevant documents or records. Interview: Contractor personnel with information system media protection and storage responsibilities.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Media Protection	Media Protection	SR-347	The Contractor must protect and control media containing EC MAN/WAN Services Data during transport outside of controlled areas by developing and implementing a process to be approved by EC that adheres to the guidance set out in the TBS Operational Security Standard on Physical Security and the RCMP G1-009, Transport and Transmittal of Protected and Classified Information. The Contractor must maintain accountability for media containing EC MAN/WAN Services Data during transport outside of controlled areas. The Contractor must restrict and document the activities associated with transport of media containing EC MAN/WAN Services Data to authorized personnel.	Examine: secure SDLC artefacts - EC MAN/WAN Services system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; EC MAN/WAN Services system media; other relevant documents or records. Interview: Contractor personnel with information system media protection and storage responsibilities.	Completeness, Effectiveness, Reliability	No	
Media Protection	Media Protection	SR-351	The Contractor must track, control and verify media sanitization by: a) performing media sanitization in compliance with ITSG- 06 (http://www.cse-cst.gc.ca/its-sti/publications/itsg- csti/itsg06-eng.html) requirements for Secret information; b) recording media sanitization actions; c) testing sanitization equipment and procedure to verify correct performance at least annually; and d) sanitizing re-allocated used storage devices prior to connecting them to the EC MAN/WAN Service Contractor Infrastructure.	Examine: secure SDLC Artefacts - EC MAN/WAN Services system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; EC MAN/WAN Services system audit records; other relevant documents or records. Interview: Contractor personnel with information system media sanitization responsibilities.	Completeness, Effectiveness, Reliability	No	
Physical Security	Physical & Environmental Protection	SR-357	The EC MAN/WAN Services Network Operations and EC MAN/WAN Services Security Operations must be in a secure area (floor, room or cage) dedicated to EC with physical security and electronic monitoring controls that allow access only to authorized Contractor personnel. The Contractor may include the Contractor OAM Zone within the secure area dedicated to EC, subject to personnel clearances in compliance with the EC MAN/WAN Services SRCL and Operator role assignments in compliance with SR-139.	Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; EC MAN/WAN Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. Interview: Contractor personnel with physical access control responsibilities. Test: Physical access control capability; physical access control devices.	Completeness, Effectiveness, Reliability	No	
Policy & Procedures	Physical & Environmental Protection	SR-358	The Contractor must conduct an annual review of the physical and environmental protection policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Physical and environmental protection policy and procedures; other relevant documents or records. Interview: Contractor personnel with physical and environmental protection responsibilities.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Physical Security	Physical & Environmental Protection	SR-362	The Contractor must control access to EC MAN/WAN Services Security Operations or EC MAN/WAN Services Network Operations facilities that includes: a) monitoring access 24 hours per day, 7 days per week; b) enforcing access authorizations for all entry/exit points to the Contractor's facilities, excluding those areas within the facility officially designated as publicly accessible; c) verifying individual access authorizations before granting access; d) controlling entry using access control devices with electronic monitoring and/or the use of security personnel; e) controlling access to areas officially designated as publicly accessible in accordance with the Contractor's assessment of risk; f) securing keys, combinations, and other physical access devices; g) conducting inspection of access control devices on an annual basis; and h) changing combinations and/or replacing locks immediately when combinations are compromised, keys are lost or individuals are transferred or terminated.	Examine: secure SDLC artefacts - EC MAN/WAN Services physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; EC MAN/WAN Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. Interview: Contractor personnel with physical access control responsibilities. Test: ST&E test results demonstrating physical access control capability; physical access control devices.	Completeness, Effectiveness, Reliability	No	
Physical Security	Physical & Environmental Protection	SR-366	The Contractor must design its EC MAN/WAN Services Facilities with equipment redundancy, alternative power sources and alternative routing. The Contractor must protect telecommunications cabling from unauthorized interception and damage. The Contractor must control access to telecommunications wiring, spaces and pathways (i.e., telecommunications rooms, main terminal rooms and other equipment rooms) in a manner appropriate for the sensitivity level of the information being transmitted.	Examine: secure SDLC artefacts - EC MAN/WAN Services physical and environmental protection policy; procedures addressing access control for transmission medium; EC MAN/WAN Services system design documentation; facility communications and wiring diagrams; other relevant documents or records.	Completeness, Effectiveness, Reliability	No	
Physical Security	Physical & Environmental Protection	SR-372	The Contractor must review visitor access records to its EC MAN/WAN Services Facilities every 90 days and must initiate a Security Incident Ticket upon discovery of abnormal activity.	Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; EC MAN/WAN Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. Interview: Contractor personnel with physical access control responsibilities. Test: Physical access control capability; physical access control devices.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Physical Security	Physical & Environmental Protection	SR-374	The Contractor must protect power equipment and power cabling for EC MAN/WAN Services from damage and destruction.	Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; EC MAN/WAN Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. Interview: Contractor personnel with physical access control responsibilities. Test: Physical access control capability; physical access control devices.	Completeness, Effectiveness, Reliability	No	
Physical Security	Physical & Environmental Protection	SR-375	The Contractor must implement protection devices to prevent the accidental activation of emergency power shutoff mechanisms of EC MAN/WAN Services Contractor Infrastructure.	Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; EC MAN/WAN Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. Interview: Contractor personnel with physical access control responsibilities. Test: Physical access control capability; physical access control devices.	Completeness, Effectiveness, Reliability	No	
Personnel Security	Personnel Security	SR-402	Upon termination of an individual employed by the Contractor that was associated with EC MAN/WAN Services, the Contractor must prior to announcement of the termination: a) terminate physical access to EC MAN/WAN Services facilities for the employee; b) terminate EC MAN/WAN Services Contractor Infrastructure access for the employee: c) terminate Remote Access to EC MAN/WAN Services Contractor Infrastructure for the employee; and d) retrieve all security-related property (e.g., employee identity card, physical authentication token) from the employee.	Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records. Interview: Contractor personnel with personnel security responsibilities.	Completeness, Effectiveness, Reliability	No	
Personnel Security	Personnel Security	SR-404	The Contractor must use access agreements for the EC MAN/WAN Services Infrastructure and EC MAN/WAN Services Data where: a) prior to being granted access to the EC MAN/WAN Services Infrastructure and/or EC MAN/WAN Services Data, Operators must sign the access agreement that includes the formal sanctions process that applies for failing to comply with the terms and conditions of the access agreement, and b) the Contractor reviews and updates access agreements to the EC MAN/WAN Services Infrastructure and EC MAN/WAN Services Data every two years.	Examine: Signed access agreement from ESP.	Compliance	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Personnel Security	Personnel Security	SR-407	The Contractor must provide semi-annual training for Operators on their responsibilities to protect the privacy and confidentiality of the EC MAN/WAN Services Data and Client Data and the sanctions for failure to comply.	Examine: Signed access agreement from Contractor training records for protection of privacy and confidentiality of EC MAN/WAN Services data.	Compliance	No	
Infrastructure	System & Services Acquisition	SR-127	The Contractor must use firewall appliances that have been validated: a) to at least EAL-4 under a recognized Common Criteria scheme. Products that have been validated in EC are described at http://www.cse-cst.gc.ca/its- sti/services/cc/index-eng.html; or b) against a Protection Profile meeting a conformance claim for medium robustness environments, as defined by the Common Criteria Evaluation & Validation scheme.	Examine: Development/Installation/Operational Artefacts - System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for EC MAN/WAN Services systems or services; other relevant documents or records. Interview: Contractor personnel with EC MAN/WAN Services system security, acquisition, and contracting responsibilities.	Completeness, Effectiveness, Reliability	No	
Policy & Procedures	System & Communications Protection	SR-408	The Contractor must conduct an annual review of the system and communications protection policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Development/Installation/Operational Artefacts - System and communications protection policy and procedures; other relevant documents or records Interview: Contractor personnel with system and communications protection responsibilities.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Boundary Protection and Zoning	SR-109	The Contractor must ensure the Boundary Protection for the EC MAN/WAN Security Operations Zone and EC MAN/WAN Network Operations Zone are from different vendors than those implemented for Boundary Protection with the Internet.	Examine: secure SDLC artefacts - EC MAN/WAN Services system and communications protection policy; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; list of technologies deployed in the EC MAN/WAN Services system; acquisition documentation; acquisition contracts for EC MAN/WAN Services system components or services; other relevant documents or records. Interview: Contractor personnel with information system acquisition, development, and implementation responsibilities.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Communications Protection	SR-415	The Contractor must connect EC MAN/WAN Services Contractor Infrastructure to external networks or information systems that have been approved by EC, and only through Boundary Protection in compliance with SR-100 to SR-106 inclusive.	Examine: Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing boundary protection; traffic flow policy; EC MAN/WAN Services system security architecture; EC MAN/WAN Services system design documentation; boundary protection hardware and software; EC MAN/WAN Services system architecture and configuration documentation; EC MAN/WAN Services system configuration settings and associated documentation; records of traffic flow policy exceptions; other relevant documents or records. Interview: Contractor personnel with boundary protection responsibilities. Test: ST&E test results that demonstrate managed interfaces implementing organizational traffic flow policy.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	System & Communications Protection	SR-417	The Contractor must manage the Boundary Protection for EC MAN/WAN Services Network Security Zones as follows: a) deny all network traffic by default; b) define allowable traffic for each boundary (i.e. deny all, permit by exception); c) terminate the connection associated with a communications session at the end of the session, or after a configurable number of minutes of inactivity specified by EC; d) monitor traffic for unusual or unauthorized activities or conditions; e) generate a Security Incident Ticket for detected unusual or unauthorized activities or conditions; e) as necessary, monitor traffic at selected interior points within the security zone (e.g., subnets, subsystems) to detect anomalies; and f) monitor and control changes to the Boundary Protection traffic flow configuration settings in accordance with the EC MAN/WAN Services Configuration Management Plan.	Examine: Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing boundary protection; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system hardware and software; EC MAN/WAN Services system architecture; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; other relevant documents or records. Test: ST&E test results demonstrate mechanisms implementing managed interfaces within information system boundary protection devices.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Communications Protection	SR-420	The Contractor must prevent EC MAN/WAN Services Contractor Infrastructure from communicating outside of approved Network Security Zone communication paths (e.g. accessing the Internet via a separate connection available to the device).	Examine: secure SDLC artefacts - EC MAN/WAN Services system and communications protection policy; procedures addressing boundary protection; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system hardware and software; EC MAN/WAN Services system architecture; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Test: ST&E test results demonstrating automated mechanisms supporting non-remote connections with the EC MAN/WAN Services system; Mechanisms implementing managed interfaces within EC MAN/WAN Services system boundary protection devices.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Communications Protection	SR-422	The Contractor must detect unauthorized exfiltration of EC MAN/WAN Services Data through the Service Portal in real time.	Examine: Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing boundary protection; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; other relevant documents or records. Test: ST&E test results that demonstrate automated mechanisms preventing unauthorized exfiltration of information across managed interfaces.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	System & Communications Protection	SR-424	The Contractor must monitor host/server behaviours in real-time to detect attacks and evidence of compromise (e.g., Host-based Intrusion Detection and Prevention) of EC MAN/WAN Services.	Examine: Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing boundary protection; EC MAN/WAN Services system design documentation; boundary protection hardware and software; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Test: ST&E test results that demonstrate automated mechanisms implementing host-based boundary protection capability.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Communications Protection	SR-427	The Contractor must protect the integrity and confidentiality of EC MAN/WAN Services Security Data, GCNet WAN Services SDP Device Configuration Data and a EC MAN/WAN Services Internetwork Operational Configuration during transmission across a network and, unless otherwise approved by EC, must use Communications Security Establishment EC- approved cryptographic modules and algorithms in compliance with SR-20.	Examine: Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing transmission integrity; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Test: ST&E test results that demonstrate cryptographic mechanisms implementing transmission integrity capability within the EC MAN/WAN Services system.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Communications Protection	SR-441	The Contractor must approve Mobile Code used in the EC MAN/WAN Services and must deny any other Mobile Code from being downloaded and executed.	Examine: Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; other relevant documents or records. Interview: Contractor personnel with mobile code authorization, monitoring, and control responsibilities. Test: ST&E test results to demonstrate mobile code authorization and monitoring capability for the organization.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Communications Protection	SR-446	The Contractor must prohibit the installation and use of VoIP technologies within the EC MAN/WAN Services Security Operations Zone and EC MAN/WAN Services Network Operations Zone, unless otherwise approved by EC.	Examine: Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; other relevant documents or records. Interview: Contractor personnel with VoIP authorization and monitoring responsibilities. Test: ST&E test results that demonstrate VoIP authorization and monitoring capability for the organization.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Communications Protection	SR-449	The Contractor must invalidate session identifiers for EC MAN/WAN Services Infrastructure, that is accessible using Internet Protocol, upon Operator logout or Remote Management session termination.	Examine: secure SDLC artefacts - EC MAN/WAN Services System and communications protection policy; procedures addressing session authenticity; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Test: ST&E test results demonstrating automated mechanisms generating and monitoring unique session identifiers for EC MAN/WAN Services.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	System & Communications Protection	SR-451	EC MAN/WAN Services Contractor applications that use stateless protocols (e.g. HTTP) must: a) generate a unique session identifier for each session with randomness using CSEC-approved cryptography per SR-20; and b) recognize only session identifiers that are generated by the EC MAN/WAN Services Contractor Infrastructure.	Examine: secure SDLC artefacts - EC MAN/WAN Services System and communications protection policy; procedures addressing session authenticity; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Test: ST&E test results demonstrating automated mechanisms generating and monitoring unique session identifiers for EC MAN/WAN Services.	Completeness, Effectiveness, Reliability	No	
Policy & Procedures	System & Information Integrity	SR-457	The Contractor must conduct an annual review of the system and information integrity policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Development/Installation Artefacts - EC MAN/WAN Services system and information integrity policy and procedures; other relevant documents or records; Interview: Contractor personnel with system and information integrity responsibilities.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Information Integrity	SR-458	The Contractor must implement patch management of custom software for EC MAN/WAN Services Contractor Infrastructure that includes: a) identifying, reporting, and correcting flaws in the custom software; b) testing software updates related to flaw remediation for effectiveness and potential side effects on the EC MAN/WAN Services before installation; and incorporating flaw remediation into the EC MAN/WAN Services configuration management process.	Examine: Development/Installation Artefacts - EC MAN/WAN Services system and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the EC MAN/WAN Services system; list of recent security flaw remediation actions performed on the EC MAN/WAN Services system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct EC MAN/WAN Services system flaws); test results from the installation of software to correct EC MAN/WAN Services system flaws; other relevant documents or records; Interview: Contractor personnel with flaw remediation responsibilities.	Completeness, Effectiveness, Reliability	No	
Security Operations	Security Monitoring	SR-468	The Contractor must continuously monitor EC MAN/WAN Services Contractor Infrastructure, that is accessible using Internet Protocol, to: a) detect attacks, Incidents and abnormal events; b) identify unauthorized use and/or access to Client Data, EC MAN/WAN Services Data; and c) respond, contain, and recover from threats and attacks against the EC MAN/WAN Services. The Contractor must heighten the level of monitoring activity for EC MAN/WAN Services Contractor Infrastructure whenever there is an indication of increased risk to EC MAN/WAN Services as identified by the Contractor or by EC.	Examine: Development/Installation Artefacts - information system design documentation; information system monitoring tools and techniques documentation; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system protocols documentation; Examine: Operational Artefacts- System and information integrity policy; procedures addressing EC MAN/WAN Services system monitoring tools and techniques; other relevant documents or records]. Interview: Contractor personnel with EC MAN/WAN Services system monitoring responsibilities. Test: ST&E test results demonstrating automated tools supporting near real-time event analysis.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	System & Information Integrity	SR-471	The EC MAN/WAN Services Contractor Infrastructure, that is accessible using Internet Protocol, must automatically generate real-time alerts (e.g. using correlation rules) following indications of compromise.	Examine: secure SDLC artefacts - EC MAN/WAN Services System and information integrity policy; procedures addressing EC MAN/WAN Services system monitoring tools and techniques; EC MAN/WAN Services system monitoring tools and techniques documentation; EC MAN/WAN Services system configuration settings and associated documentation; other relevant documents or records. Test: ST&E test results demonstrating EC MAN/WAN Services system monitoring real-time alert capability as per SR-471.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Information Integrity	SR-474	The Contractor must protect Client Data, EC MAN/WAN Services Data and audit logs from unauthorized access, modification, and deletion.	Examine: secure SDLC artefacts - EC MAN/WAN Services system audit and accountability policy; procedures addressing content of audit records; EC MAN/WAN Services system design documentation; list of EC MAN/WAN Services system-defined auditable events; EC MAN/WAN Services system configuration settings and associated documentation; EC MAN/WAN Services system audit records; other relevant documents or records. Test: ST&E test results demonstrating the automated mechanisms implementing centralized management and analysis of log content as per SR-474.	Completeness, Effectiveness, Reliability	No	
Infrastructure	System & Information Integrity	SR-483	The Contractor must implement a centrally managed integrity verification solution to detect unauthorized changes to the EC MAN/WAN Services Data, the EC MAN/WAN Services Security Operations infrastructure and EC MAN/WAN Services Network Operations infrastructure by: a) performing integrity scans on a weekly basis or as specified by EC, and b) automatically generating a Security Incident Ticket upon discovering discrepancies during integrity verification.	Examine: Development/Installation Artefacts - System and information integrity policy; procedures addressing software and information integrity; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records]. Examine: Operational Artefacts - System and information integrity policy; procedures addressing software and information integrity; security plan; EC MAN/WAN Services system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; EC MAN/WAN Services system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records. Test: ST&E test results will verify and validate software integrity protection and verification capability.	Completeness, Effectiveness, Reliability	No	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Infrastructure	System & Information Integrity	SR-492	The Contractor must implement input validation for EC MAN/WAN Services applications where possible.	Examine: Development/Installation Artefacts - documentation for automated tools and applications to verify validity of information; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; Examine: Operational Artefacts - System and information integrity policy; procedures addressing information validity; access control policy and procedures; separation of duties policy and procedures; other relevant documents or records. Test: ST&E test results provide EC MAN/WAN Services system capability for checking validity of information inputs.	Completeness, Effectiveness, Reliability	No	
Infrastructure	Access Control	SR-659	The Service Portal must include: User account password expiry and recovery as follows: <SR-659> i) issue a challenge question when a User's password is forgotten. If the User correctly answers the challenge question, the Contractor must send a new password to the User by e-mail, and must not provide it over the telephone; ii) one-time temporary passwords for enrolment and password recovery subject to a configurable validity period, as specified by EC; and iii) automatic advanced notification of pending password expiry as specified by EC.	Examine: secure SDLC artefacts - EC MAN/WAN Services system identification and authentication policy; procedures addressing user identification and authentication; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records. Test: ST&E tests demonstrate automated mechanisms implementing identification and authentication capability for Level 2 Assurance as described in ITSG-31 for the EC MAN/WAN Services system.	Completeness, Effectiveness, Reliability	Yes	
Infrastructure	Access Control	SR-663	The Service Portal must log the following transactions for Level 3 Assurance, as detailed in ITSG-31: <SR-663> i) password changes; ii) credential registrations; iii) password recovery; iv) expired credentials; v) authenticated User sessions; and vi) denied User sessions, including indication of from an invalid or inactive account.	Examine: secure SDLC artefacts - EC MAN/WAN Services system audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; EC MAN/WAN Services system audit records; EC MAN/WAN Services system incident reports; other relevant documents or records. Test: ST&E test results demonstrating automated mechanisms implementing EC MAN/WAN Services system auditing of auditable events as per SR- 663.	Completeness, Effectiveness, Reliability	Yes	

Requirement Category	Requirement Sub-Category	Security ID	Security Requirement	Assessment Method	Assessment Criteria	SOW Trace	Contractor Deliverable
Configuration Management	Change Management	SR-696	The Contractor must assess the security impact of changes to EC MAN/WAN Services Infrastructure by: a) analyzing new software before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice; b) informing EC of potential security impacts prior to change implementation, and c) checking the security functions, after changes are implemented, to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the applicable security requirements.	Examine: secure SDLC phases - Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the EC MAN/WAN Services system; EC MAN/WAN Services system design documentation; EC MAN/WAN Services system architecture and configuration documentation; other relevant documents or records; Interview: Contractor personnel with configuration change control responsibilities;	Completeness, Effectiveness	No	
Policy & Procedures	Risk Assessment	SR-577	The Contractor must conduct an annual review of the risk assessment policies and procedures published in the EC MAN/WAN Services Operational Security Procedures document approved by EC. The Contractor must update the Operational Security Procedures in compliance with SR-552.	Examine: Development/Installation Artefacts - EC MAN/WAN Services system and information risk assessment policy and procedures; other relevant documents or records; Interview: Contractor personnel with risk assessment responsibilities.	Completeness, Effectiveness, Reliability	No	

Metropolitan Area Network and Wide Area Network Services

Annex B

Questions to Industry

Questions to Industry

1. Are the requirements elaborated in the draft statement of work and related appendices attached to this request for information (RFI) consistent with what can be delivered by industry?

2. Based on the information provided regarding Election Canada's (EC's) requirements, do you recommend EC forego requirements for layer 2 metropolitan area network (MAN) services, as described in part II of the attached draft Annex A – Statement of Work, pursuing instead Multiprotocol Label Switching (MPLS) services, as described in part III of the attached draft Annex A – Statement of Work, for EC's MAN/wide area network (WAN) requirements outlined in section 4 of the attached draft Annex A – Statement of Work? Please provide a rationale (e.g. pros and cons of each type of service) for your recommendation.

3. Based on the detailed information provided regarding EC's security requirements, do you foresee major challenges, issues or risks? What could EC do to address these challenges or issues or to mitigate the risks associated with those issues and challenges you may have identified?

4. Generally speaking and based on the information provided by EC in the RFI documentation, do you foresee any barriers, impediments or showstoppers in responding to this solicitation or for EC to successfully meet its MAN/WAN service requirements?

5. Based on previous procurements and by providing examples, can you identify what evaluation criteria should be used by EC in order to align our requirements with industry best practices and current trends?

6. Based on previous procurements, can you provide any suggestions that, in your opinion, could assist EC in the development of the basis of selection?