Service | Innovation | Value

Shared Services Canada

Annex A-1 Statement of Work
General

Enterprise Contact Centre Services (ECCS)

Table of Contents

Index of Tables

1 PROJECT MANAGEMENT

(1) The requirements in this section apply to any Work for Service Readiness, Security and Privacy Readiness and Service Implementation.

1.1 Service Project

(2) When and as requested by Canada, the Contractor must conduct and complete portions of the Work as a Service Project.

(3) The Contractor must begin the Work identified by Canada as a Service Project within 10 FGWDs of the request by Canada.

1.1.1 Service Project Meetings

(4) The Contractor must facilitate a weekly meeting for each Service Project (Service Project Meeting) that includes a Powerpoint presentation to review:

a) minutes from the previous Service Project Review Meeting and approval by Canada;

b) content of the Service Project Review Meeting Report; and

c) action items log (open and closed).

(5) The Contractor must facilitate a weekly meeting to review all Service Projects (Project Management Office Meeting) that includes a Powerpoint presentation to review:

a) minutes from the previous PMO Meeting and approved by Canada;

b) the content in the PMO Status Report; and

c) action items log (open and closed).

1.1.2 Service Project Reporting

(6) The Contractor must provide the reports for Service Projects in Table 1.

Table 1. Service Project Reports

Report Name	Service Project Status Report
Frequency	2 FGWDs prior to each Service Project Review Meeting
Purpose	The report must present the status of a Service Project.
Description	The report must include: a) minutes from the previous Service Project Review Meeting; b) graphical and tabular view of Project Schedule milestones including: i) planned/actual completion dates; ii) current/previous forecasted completion dates; iii) Work dependencies within the Service Project and with other Service Projects; and iv) Identification of critical path Work activities. c) current and upcoming Work tasks; d) project issues including assessment of impacts and current escalation status; e) summary of Service Project risks;

	f) summary with description of the Project Change Requests including: i) approved by Canada in the preceding week; ii) currently require approval by Canada; g) summary of the Project Variances including: i) approved by Canada in the preceding week; ii) currently require approval by Canada; and iii) resulted in a Project Change Request.
Report Name	Project Management Office (PMO) Status Report
Frequency	2 FGWDs prior to each PMO Meeting
Purpose	The report must present an overall summary of all Service Projects.
Description	The report must include: a) minutes from the previous PMO Meeting; b) summary of top 5 issues; c) view of Master Project Schedule milestones including: i) planned/actual completion dates; ii) current/previous forecasted completion dates; iii) Work dependencies within the Service Project and with other Service Projects; and iv) Identification of critical path Work activities. d) action items log (open and closed).

1.2 Project Change Requests

(7) The Contractor must create and maintain a log of Project Change Requests for each Service Project and master log for all Service Projects where the format of the log is developed in consultation with Canada and approved by Canada.

(8) The Contractor must review each Project Change Request in consultation with Canada and assess the impacts.

(9) The Contractor must update the Project Schedule if a Project Change Request affects any task or timeline in the Service Project.

(10) Canada is not required to issue a Project Change Request for new Service Projects. The re-allocation of Work between existing Service Projects or between existing Service Projects and new Service Projects will be done in consultation with the Contractor.

1.3 Project Variances

(11) The Contractor must create and maintain a log of Project Variances for each Service Project and master log that summarizes the Project Variances for all Service Projects where format of the log is developed in consultation with Canada and approved by Canada.

(12) A Project Variance does not relieve the Contractor from meeting the schedule for a Service Project.

(13) The Contractor must review each Project Variance in consultation with Canada and assess the impact on the Service Project. Any actions required, or changes that affect the scope, cost, or delivery dates for the Service Project must be managed through the Project Change Request process.

1.4 Project Risk Register

(14) The Contractor must create and maintain a Project Risk Register for each Service Project and a master register that summarizes the risks for all Service Projects where the format of the register is developed in consultation with Canada and approved by Canada...

1.5 Project Schedule

(15) The Contractor must create and maintain a Project Schedule for each Service Project and a master schedule that summarizes the Project Schedules for all Service Projects where the format of the schedule is developed in consultation with Canada and approved by Canada.

(16) .A Project Schedule must:

a) not create dependencies on Canada's review and acceptance of Work, unless approved by Canada;

b) limit dependencies to the maximum extent possible;

c) schedule tasks in parallel to the maximum extent possible;

d) provide for deliverables to be submitted progressively (i.e. not all at once);

e) be produced and maintained in Microsoft Project;

f) identify the phases, gates, deliverables and milestones of the Work including:

i) identification of tasks representing tangible deliverables with deliverable numbers assigned that correlates with the numbering and description of deliverables in the Project Plan;

ii) identification of responsibility for each task;

iii) duration of each task;

iv) start and end dates for each task, including baseline, forecast, and actual dates; and

v) percentage complete for each task; and

g) identify any Project Change Requests and Project Variances that cause changes to the completion date of any major milestone, with numbers assigned that correlate with the numbers assigned to them in the Service Project Status Report.

(17) The Contractor must set a baseline for all task start and end dates in a Project Schedule based on the date of acceptance of the Project Schedule by Canada.

(18) The Contractor must not change the baseline of a Project Schedule for the duration of the Service Project unless approved by Canada. If a change to the Project Schedule is approved by Canada, the Contractor must set a new baseline schedule in a new version of the Project Plan that clearly states that the baseline has been revised.

(19) The Contractor must ensure that resource assignments for a Project Schedule take into consideration the availability and non-availability of each resource (e.g. holidays, training and vacation), such that there is no impact to the completion of Work in the Service Project.

1.6 Project Resource Plan

(20) The Contractor must create and maintain a Project Resource Plan for each Service Project that includes:

a) roles and responsibilities of all resources (primary and backup Key Resources, other resources to the Manager level) to complete the Work for the Service Project including:

i) name and title of the resource;

ii) description of the qualifications of the resource to complete the Work; and

iii) work level allocation (dedicated, part time);

b) a Responsible, Accountable, Consulted, and Informed (RACI) chart to identify the Work by deliverable and Work activities to be completed by each resource, Canada and Client stakeholders to the manager level;

c) summary assessment of why the identified resources (number and qualifications) are sufficient to complete the Work in accordance with the approved schedules taking into consideration the availability (e.g., holidays, training and vacation) and location of each resource; and

d) a description of the management escalation process (org chart with names and contact information for all resources on the Service Project).

(21) The Contractor must create and maintain a master Project Resource Plan that summarizes the Project Resource Plans for all Service Projects.

1.7 Executive Steering Committee

(22) The Contractor must participate in a Senior Executive Steering Committee, with meetings to be held monthly until the end of Service Readiness. The Committee will assess progress on the Service Projects, the completion of Service Readiness, provide guidance on matters escalated by either Canada or the Contractor and foster collaboration between Canada and the Contractor.

2 KEY RESOURCES

(23) The Contractor must provide the Key Resources listed in Table 2 to perform the Work Responsibilities and other roles as the need arises. These individuals must have the Number of Years of Basic Experience and the Basic Experience described in the table.

(24) Unless otherwise indicated and approved by Canada, all Key Resources must be accessible from 7 am to 7 pm ET during FGWDs using communication methods approved by Canada.

(25) The Contractor must ensure there are sufficient back-up resources for all Key Resources for work outside the core working hours of 9 am to 5 pm ET during FGWDs. Where Key Resources are unavailable during the core working hours, back-up resources must be available.

(26) Given the role of the Service Operations Manager in relation to escalation of Incidents, the Service Operations Manager must be accessible to Canada 24 hours per day, 7 days per week and 365 days per year for that purpose. Given the nature of this role, the Contractor may name back-up Service Operations Managers, in order to ensure coverage during off-hours.

Table 2 Key Resource Work Responsibilities

Key Resource	Work Responsibilities	Number of Years of Basic Experience	Basic Experience
Project Manager	a) be Canada's single point of contact for a Service Project; b) facilitate Service Project Review meetings; c) coordinate the Work activities of a Service Project; d) identify, track, document, prioritize and escalate issues for a Service Project; e) create and maintain a log of Project Change Requests for a Service Project; f) create and maintain a log of Project Variances for a Service Project; g) create and maintain a Project Resource Plan for a Service Project; h) create and maintain a Project Schedule for a Service Project; i) create and maintain a Project Risk Register for a Service Project; and j) create and maintain a Service Project Status Report for a Service Project.	5	a) managing the identification, prioritization, escalation and resolution of project issues for projects; b) managing the identification, prioritization, escalation and resolution of Project Change Requests and Project Variances; c) tracking Project Risks; d) creating and maintaining project schedules; e) creating and maintaining project status reports; and f) managing project teams.
Service Operations Manager	a) point of contact and liaison for the IT Service Management b) point of contact for escalation and resolution of Incidents; c) point of contact and liaison for managing the tracking, prioritization, escalation and implementation of Service Orders; d) facilitate clarification and reconciliation of invoices e) facilitate communications and integration with Canada's Service Desk. f) facilitate Service Management Review meetings;	5	a) managing the escalation and resolution of service management and service delivery issues; b) managing the prioritization, escalation and implementation of Service Orders; c) managing the escalation and resolution of Incidents;

	g) facilitate discussions for Outage Time review and Service Credit reconciliation		
Enterprise Architect	a) be Canada's point of contact for the engineering, design and architecture of Enterprise Contact Centre Services; b) be Canada's point of contact and liaison for security design and architecture of Enterprise Contact Centre Services; c) document and analyze Canada's requirements, assess the impacts to Enterprise Contact Centre Services and recommend changes, upgrades, and functional enhancements; d) facilitate Design and Engineering meetings and any technical working groups;	5	a) planning, designing and engineering of Services; b) analyzing client requirements and assessing impacts to Services; and c) identifying and recommending changes, upgrades, and functional enhancements to Services.
Security Manager	a) be Canada's point of contact for managing the identification, prioritization, escalation and resolution of Security Incident Tickets: b) facilitate Security meetings;	5	a) managing the identification, prioritization, escalation and resolution of Security Incident Tickets;

3 DOCUMENTATION

(27) The Contractor must define the content and format of documents for deliverables in:

a) in consultation with Canada and subject to Canada's acceptance;

b) English, and in French when requested by Canada;

c) the native format (e.g. Word, Excel, Visio) and in PDF in a format. Where the diagrams are embedded within another document format (e.g. Word), the diagrams must be in a metafile format (not editable) to reduce the size of the documents;

(28) The Contractor must provide all diagrams used for a document as native Visio diagrams to Canada within 5 FGWDs of a request from Canada.

(29) The Contractor must provide user guides, training materials and OEM documentation in both English and French.

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

(31) Unless otherwise specified, all documents must be accessible on the Service Portal throughout the Contract Period by searching and sorting documents based on any date range, status (new, authorized, in progress, completed), and type.

(32) All documents must be downloadable from the Service Portal with a file name and COTS format selected by the User, where the COTS format can include:

a) HTML;

b) PDF; and

c) Microsoft application (Word, Excel, Powerpoint etc).

(33) The Contractor must not make any changes (format, content provided) to an approved deliverable without following the Request Fulfillment processes.

(34) The Contractor must provide an updated deliverable (text and diagrams) to Canada within 20 FGWDs of a request by Canada that reflects all changes to the document in associated Service Requests since the last version of the document.

4 MEETINGS

(35) Meetings must be conducted during business hours (8 am to 5 pm ET) on FGWDs.

(36) The Contractor must provide agendas for all meetings no later than 1 FGWD prior to the meeting (excluding daily meetings) unless otherwise approved by Canada.

(37) Except where Canada specifies otherwise, for each meeting attended by the Contractor, the Contractor is responsible for:

a) coordinating with Canada;

b) coordinating any subcontractor participation (if necessary);

c) providing the agenda, minutes, schedules, lists, tests, design analysis and any other pre- and post-review data as appropriate;

d) ensuring that qualified Contractor personnel with knowledge of the issues to be discussed attend the meeting; and

e) ensuring the Contractor personnel representatives have sufficient authority to make expeditious decisions on behalf of the Contractor.

(38) The Contractor must prepare minutes for each meeting during the meeting and review with Canada for acceptance at the end of the meeting where format for minutes is developed in consultation with Canada and approved by Canada.

5 SERVICE READINESS

(39) The Work in this subsection must be completed by the Contractor and accepted by Canada for the Service Readiness deliverable.

5.1 Operation and Management Service Design

(40) The Contractor must provide an Operations Administration and Management Service Design (OAMSD) in accordance with the requirements in the SOW and resulting Contract with the following subsections:

a) Service Desk;
b) Service Portal;
c) Operations Centre;
d) IT Service Management;
e) Reporting;
f) Billing and Invoicing (refer to Billing and Invoicing in the Contract); and
g) Service Provisioning (refer to Service Provisioning in the Contract).

(41) The OAMSD must include for each subsection:

a) management and operational structure and organization including the roles and responsibilities of key personnel and subject matter experts performing Work under this Contract;
b) operational and management escalation processes that include:
    i) the identification of the designated Canada and Contractor personnel authorized to invoke the escalation procedure;
    ii) the escalation contact names, titles, email addresses and phone numbers;
    iii) the escalation time frames based on length of time, priority and impact; and
c) detailed diagrams and swim lanes illustrating the processes where applicable.

(42) The OAMSD must include a detailed user interface design for the Service Portal and description of all user interaction flows with page mock-ups or screen captures that illustrate the use of and access to the Service Portal for:

a) IT Service Management
b) Service Provisioning (refer to Service Provisioning in the Contract);
c) Reporting;
d) Billing and Invoicing (refer to Billing and Invoicing in the Contract);
e) Documentation; and
f) Canada's administration of Services.

(43) The OAMSD must include the following for each report:

a) wireframe that shows the report as viewed and utilized by the User;
b) data dictionary (refer to subsection Data Dictionary for required information); and
c) location of report on the Service Portal.

5.2 Technical Service Design

(44) The Contractor must provide a Technical Service Design (TSD) in accordance with the requirements in the SOW and resulting Contract with the following subsections:

a) design and architecture overview including:
    i) logical and physical diagrams for ECCS Infrastructure;
    ii) integration with Canada Services specified by Canada;
    iii) locations of the Contractor SDPs;
b) detailed design and architecture including:

i) Integration with Canada Services specified by Canada;
ii) Naming and Addressing;
iii) Quality of Service; and
iv) Interoperability;

c) how the service design requirements (see subsections to this section) for the Service are to the implemented;
d) the hardware and software components (make, model, release, etc.) to be implemented at a Canada SDPs and Contractor SDPs where applicable;
e) the configuration details for individual ECCS requirements, functions and features as selected by Canada from the SOW;
f) the connection and operation with other Services;
g) the connection and operation with Canada Services specified by Canada including:
i) technical and configuration requirements for the Canada Services;
ii) signaling and media port numbers and IP addresses; and
iii) network bandwidth.

5.3 User Operation Guide

(45) The Contractor must provide a User Operations Guide that describes the use and operation of ECCS for ECCS Users that includes as a minimum:

a) User account administration;
b) login procedures;
c) assigning Skillsets, APL and Call Presentation parameters to Agents;
d) managing Skillsets schedules;
e) assigning Agents to Team Leaders;
f) assigning CPL to Call Types;
g) reporting;
h) creating custom historical data reports; and
i) creating and activating recorded announcements.

5.4 Training Modules

(46) The Contractor must provide the ECCS Training Modules in Table 3 with content developed in consultation with Canada and also approved by Canada. This content constitutes “Material” in accordance with Section 20 (Copyright) in the General Conditions.

(47) The Contractor must provide a syllabus of the Training Module content for acceptance by Canada before developing the training content.

Table 3. Training Modules

Training Module	Content of Training Module
Service Management	a) Service Monitoring and Reporting; b) Event and Incident Management; c) Change Management; d) Request Fulfillment; e) Release Management;

Training Module	Content of Training Module
	f) Problem Management; g) Configuration Management including CMDB; h) Service Desk; i) Service Provisioning; and j) Billing and Invoicing.
Service Portal	a) Overview of Service Portal; b) How to access documentation; c) How to access Incident Tickets, Service Requests, Change Request Tickets, Problem Tickets and Service Orders; d) How to access reports; and e) How to administer User accounts; f) How to export/download data, reports and documents.
Agent	a) How to use and operate Agent functions and features; b) How to login / logout; c) How to activate Not Ready, Make Busy; d) Interpreting Agent display status; e) How to produce and interpret Real-Time reports.
Team Leader	a) How to use and operate Team Leader functions and features; b) How to login / logout; c) Interpreting Agent display status; d) Enabling / disabling overflow routing; e) Modifying Application and system parameters; f) Activating / deactivating for day / night mode; and g) How to produce and interpret Real-Time reports.
ECCS Reports	a) How to produce and interpret ECCS Real-Time reports; b) How to produce and interpret ECCS Historical reports; c) How to define thresholds for data fields of Real-Time and Historical reports; and d) How to export reports using COTS file format.
Administrator	a) How to create, modify, activate, de-activate Agent and Team Leader profiles;

Training Module	Content of Training Module
	b) How to search for a profile; c) How to reset passwords.

(48) The Contractor must provide Training Module content to Canada in English and French and in the following formats:

a) PDF, with full search and print capabilities;

b) HTML 5; and

c) native file format, such that the layout and functionality of the original document is maintained (e.g., a file created in Microsoft Word is provided to SSC in the native Microsoft Word format).

6 SECURITY AND PRIVACY READINESS

(49) The Work in this subsection must be completed by the Contractor and accepted by Canada for the Security and Privacy Readiness deliverable.

6.1 Security Assessment Report

(50) The Contractor must complete a security assessment with an independent third party assurer, qualified under AICPA or CPA Canada and/or an ISO certification regime that conforms to ISO/IEC 17020 quality management system standards, at no additional cost to Canada that will prepare a Security Assessment Report that includes:

a) the legal business name of the Contractor;

b) current date and/or status of certifications and/or SOC 2 Type II report;

c) evidence to demonstrate compliance of the Service with security requirements in the Contract;

d) name and address of the third party assurer that performed the security assessment; and

e) evidence that the third party assurer is qualified under AICPA or CPA Canada, and/or ISO certification regime that conforms to ISO/IEC 17020 quality management system standard.

6.2 System Security Plan

(51) The Contractor must provide a System Security Plan (SSP) that documents the security controls in place, or planned for meeting, for the security requirements in the contract that:

a) Is consistent with the Contractor's enterprise architecture;

b) explicitly defines the authorization boundary for the Service;

c) describes relationships with or connections to other External Information Systems;

d) provides an overview of the Security Control Requirements for the Service;

e) describes the rationale for security controls including the tailoring and supplementation decisions; and

f) includes a component diagram that clearly shows the Services architecture.

6.3 Operations Security Procedures

(52) The Contractor must provide a Operations Security Procedures (OSP) that documents the following for each connection to a Service:

a) system components;

b) the interface characteristics;

c) security requirements;

d) nature of the information communicated;

e) secure configuration, installation, and operation of the Service;

f) effective use and maintenance of security functions;

g) known Security Vulnerabilities regarding configuration and use of administrative (i.e. privileged) security functions;

h) user-accessible security functions and how to effectively use those security functions;

i) methods for user interaction, which enables individuals to use the GPAS service in a more secure manner; and

j) user responsibilities for maintaining the security of the GPAS service and system components..

6.4 Service Incident Response Plan

(53) The Contractor must provide a Security Incident Response Plan that includes:

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 Security Incident response capability;

d) a high-level approach for how the Security Incident response capability fits into the Contractor's overall organization;

e) a definition of reportable Security Incidents;

f) a definition of metrics for measuring the Security Incident response capability; and

g) a definition of resources and management support needed to effectively maintain and mature the Security Incident response capability.

6.5 Vulnerability Assessment Plan

(54) The Contractor must provide a Vulnerability Assessment Plan that includes:

a) a description of the scope of the vulnerability assessment;

b) Canada witnessing arrangements;

c) a description of the vulnerability assessment process;

d) test cases where each test case includes:

i) tasks, activities, test equipment/tools used (including any software versions), and procedures that the Contractor will perform the test case;

ii) description of what is to be tested; and

iii) acceptance criteria and expected results.

6.6 Service Contingency Plan

(55) The Contractor must provide a Service Contingency Plan that describes:

a) essential missions and business functions including supporting critical GPAS system components and associated contingency requirements;

b) a detailed plan and documented processes for restoring Service operations;

c) back up strategies for datacentre facilities, network facilities, operational support systems and data, and key Service components;

d) recovery objectives, restoration priorities, and metrics as per Service Level Agreements (SLAs);

e) contingency roles, responsibilities, and assigned individuals with contact information;

f) process for full Service restoration without deterioration of the security safeguards originally planned and implemented;

g) how essential missions and business functions are maintained despite a Service disruption, compromise, or failure;

h) process(es) for testing the Service Contingency Plan;

i) detailed communications plans with Canada, Canada’s Clients and the Contractor’s suppliers and sub-contractors;

j) detailed plan and processes for transferring operational, management and administration functionality to a backup operations centre; and

k) steps the Contractor will take if any of its key subcontractors go out of business or are identified by Canada as being subject to security concerns

(56) The Contractor must implement Service Contingency Plan (all processes, procedures, roles, responsibilities etc.) following its acceptance by Canada and prior to completion of Service Readiness.

6.7 Privacy Management Plan

(57) The Contractor must provide a Privacy Management Plan to Canada that includes:

a) the roles and responsibilities of the Contractor's Privacy resources and how they interface with Canada and Contractor's suppliers;

b) a description of how the Contractor plans to develop and maintain overall privacy awareness on an ongoing basis through various channels (intranet, posters etc.);

c) a description of the Contractor's privacy protection strategies detailing exactly how the Personal Information will be treated over its life cycle;

d) a description of how the Contractor intends to ensure that its staff is trained on privacy and privacy;

e) a description of how the Personal Information will be collected, used, retained, and disclosed only for the purposes of the Work specified in the Contract;

f) a description of how the Personal Information and Records will be accessible only to authorized individuals (on a need-to-know basis) for the purposes of the Work specified in the Contract;

g) processes for the development and testing of Services without using Canada production data (i.e. real information related to Users);

h) processes to identify, document, review, report, respond, and escalate privacy related Incidents;

i) processes for managing, accessing, collecting, using, disclosing, receiving, creating or disposing of personal information;

j) processes for limiting the retention of personal information and ensuring adherence to the retention requirements of Canada, including backup and archiving of data;

k) role-based access controls to restrict/limit access to operational and administrative information required by authorized Contractor personnel including logging all instances where personnel have had access to operational information;

l) processes to ensure incorporation of specific retention and disposal requirements as determined by Canada's Privacy Impact Assessments (PIA's); and

m) processes to ensure the logging and data capture settings of the information protection and network monitoring devices are appropriately defined to limit the collection of personal information;

n) process for dealing with requests for access to Records under the Access to Information Act and requests for access to Personal Information under the Privacy Act (Access Requests).

o) the privacy breach protocol, and details on how any privacy breaches will be handled;

p) any new measures the Contractor intends to implement in order to safeguard the Personal Information and the Records in accordance with their security classification; and

q) how the Contractor intends to ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification.

(58) The Contractor must implement the Privacy Management Plan (all processes, procedures, roles, responsibilities etc.), following its acceptance by Canada and prior to completion of Service Readiness.

7 SERVICE IMPLEMENTATION

7.1 General

(59) The Contractor must implement the Services in accordance with the requirements in the Contract including but not limited to:

a) Operations Administration and Management Service Design;
b) Technical Service Design;
c) System Security Plan;
d) Security Incident Response Plan;
e) Service Continuity Plan; and
f) Privacy Management Plan

(60) The Work to integrate and operate ECCS with any of the following Canada systems and Services with a Service must be provided by the Contractor at no additional cost to Canada:

a) Canada Cellular Service;
b) Canada Long Distance Service; and
c) Canada Toll Free Service.

(61) The Contractor is responsible for and must manage and coordinate all aspects of the Work required to implement Services that minimizes impacts to Users.

(62) The Contractor must ensure that all equipment for the ECCS is applied, installed, connected, erected, cleaned, conditioned and tested in accordance with the manufacturer's directions and specifications.

7.2 Number Portability

(63) The Contractor must coordinate changes with PSTN carrier(s), including:

a) provision, implementation and testing of PSTN facilities (toll free and long distance included);
b) number portability;
c) implementation of number portability; and
d) implementation of telephone number changes and call references.

(64) The Contractor must coordinate configuration changes with the service providers of Canada Services.

7.3 Canada WAN Service at Contractor SDPs

(65) When requested by Canada, the Contractor must connect Services at Contractor SDPs to the Canada WAN Service at Canada’s cost.

(66) The Contractor must provide a continuous supply of electric power to the Canada WAN Service equipment at Contractor SDPs for a minimum of 8 hours when facility power is not available at the Contractor SDP.

(67) The Contractor must allow Canada to implement an out-of-band management connection (e.g. dial-up, dedicated connection) to the Canada WAN Service equipment at Contractor SDPs.

(68) The Contractor must provide Canada with access to the Canada WAN Services equipment at Contractor SDPs for maintenance, releases and upgrades within 5 FGWDs as requested by Canada. For emergency access related to incident investigation or outage, access must be provided within 1 hour of a request by Canada, 24 hours per day, 7 days per week, 365 days per year.

(69) The Contractor must perform a hard reset of the Canada WAN Service equipment at Contractor SDPs as directed and authorized by Canada within 15 minutes of a request by Canada 24 hours per day, 7 days per week, 365 days per year.

(70) The Contractor must provide the space (secure and controlled access, racks), cabling, power, ventilation and room temperature for the Canada WAN Service equipment at Contractor SDPs.

7.4 Services at Canada SDPs

(71) The Contractor is responsible for and must manage and coordinate all aspects of the Work required at Canada SDPs including:

a) installing cable termination equipment such as customer interface panels;

b) installing Contractor Equipment at Canada SDPs as either rack mounted (default) or shelf mounted when specified by Canada in the Service Order;

c) conducting 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;

d) implementing the Contractor Equipment within the physical location at the SDP (rack, shelf) as specified by Canada. In the event the Contractor Equipment is not implemented in the physical location specified by Canada, the implementation will be considered incomplete until the Contractor returns and relocates the equipment to the specified location at no cost to Canada;

e) labelling all Contractor Equipment and cables at each SDP using a naming convention specified by Canada; and

f) facilitating all construction of Connecting Equipment including all administration and logistics associated with any required fit-up and construction except for power, space and HVAC, including the provision and acquisition of all necessary equipment.

(72) Canada may require the Work at Canada SDPs to be performed during or after regular business hours according to the time of day specified by Canada. Business hours vary by location based on the nature of business conducted (e.g., business hours at border crossings and airports differ from tax service offices).

(73) The Contractor must not locate any of its Contractor Equipment within a Canada SDP that is used to provide services to any other customer.

(74) The Contractor must provide Canada with the method-of-procedures (MOP) specific to each SDP (where requested by Canada), developed in consultation with Canada and approved by Canada, that will be used to implement Services at an SDP a minimum of 20 FGWDs prior to the Target Delivery Date (TDD) that includes:

a) the back-out procedures to restore the original services; and

b) the schedule for the implementation activities, including Canada's testing.

(75) The Contractor must connect Contractor Equipment to Canada's equipment at a Canada SDP when approved by Canada. Canada will provide direction on the equipment and port for the connection.

(76) The Contractor must test Services in accordance with the approved ATP. The Contractor must remain at the SDP following completion of the ATP until Canada confirms that the Services are operational based on evidence provided by the Contractor.

(77) The Contractor must provide all hardware and software for acceptance testing performed by the Contractor. The Contractor must not require Canada to provide any hardware or software for acceptance testing, and must not require Canada to install any software on Canada's devices.

(78) The Contractor must use existing conduit at an SDP when directed by Canada.

(79) The Contractor must not perform any fit-up or implementation activities at a Canada SDP without prior written approval from Canada.

(80) The Contractor must allow Canada to connect/disconnect Canada's equipment to Contractor Equipment at a Canada SDP without assistance from the Contractor.

(81) The Contractor must include a network interface to connect a Service at a Canada SDP to the Canada LAN Service..

8 SERVICE OPERATIONS

(82) The Work in this subsection is applicable to the ongoing operation, administration, management and maintenance of the ECCS, with the objective of proactively diagnosing and repairing problems before these become service affecting, following:

a) approval by Canada of the Service Readiness deliverable;

b) approval by Canada of the Security and Privacy Readiness deliverable; and

c) completion of Service Implementation in accordance with initial Service Orders issued by Canada for Services.

8.1 Service Desk

(83) The Contractor must provide a Service Desk that performs the following functions:

a) acting as the primary point of contact for Incidents reported by Canada 24 hours per day, 7 days per week, 365 days per year;

b) answering and continuing the subsequent Level 1 and Level 2 dialogue using the official language of Canada (French, English) requested by the caller;

c) interacting with Canada's representatives as designated by Canada's Service Desk;

d) providing a unique and dedicated toll-free telephone number (e.g., 1-800 number) for Canada's authorized representatives to access the Service Desk; and

e) providing a single email address for Canada's authorized representatives to access the Service Desk.

8.2 Operations Centre

(84) The Contractor must provide a primary Operations Centre within Canada, with the infrastructure and resources required for the centralized management and operation of ECCS, 24 hours per day, 7 days per week, 365 days per year.

(85) 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, where the transition from the primary operations centre to the backup Operations Centre must be seamless to Canada and not affect the operations of the ECCS.

8.3 Service Review Meetings

(86) The Contractor must facilitate and conduct the Service Review meetings summarized in Table 4.

Table 4 Service Review Meetings

Meeting Name	Service Management Review Meeting
Frequency	Monthly, or as requested by Canada
Purpose	Review of Incidents, Change Requests, Service Requests, Problems, Service Level Targets and Billing/Invoicing.
Description	The meeting must include a review of: a) issues log from previous meeting; b) action items log from previous meeting; c) Post-Service Request Reports from the previous month; d) Post-Change Request Reports from the previous month;

	e) Post-Incident Reports from the previous month; f) Service Level Targets and failures from the previous month; g) Service Requests scheduled for the coming month; h) Change Requests scheduled for the coming month; i) issues that have or may affect Service performance; j) root cause analysis of open Incident Tickets; and k) root cause analysis of open Problem Tickets.
Meeting Name	Design and Engineering Review Meeting
Frequency	Within 10 FGWD of a request by Canada
Purpose	Review of engineering, design performance and capacity of Services
Description	The meeting must include a review of: a) design, engineering, performance and capacity issues; b) engineering reports (on an as requested basis); c) planned changes, upgrades and functional enhancements.
Meeting Name	Security Review Meeting
Frequency	Within 1 FGWD of a request by Canada
Purpose	Review of Security Incidents
Description	The meeting must include a review of (for each Security Incident): a) date/time and duration of Security Incident; b) description including whether attack appears to have been successful; c) scope (Service Portal; single or multiple Clients, etc.); d) estimated injury/impact level; e) list of known and suspected Applications affected; f) actions taken; g) apparent source/origin of attack(s); and h) status of mitigations.

8.4 IT Service Management

(87) The Contractor must provide IT Service Management for Services, as described in the following subsections, 24 hours per day, 7 days per week and 365 days per year.

8.4.1 Change Management

(88) The Contractor must create a Change Request for any change that may disrupt Services.

(89) All Change Requests that impact Services must be approved by Canada.

(90) The Contractor must create 1 or more Change Request Tickets for a Change Request.

(91) The Contractor must create an Emergency Change Request for each mitigation measure required to contain a Security Incident, and must implement the Emergency Change Request in accordance with the priority established by Canada for the Security Incident.

(92) The Contractor must complete the Change Request activity, excluding Emergency Change Requests, in the maintenance windows approved by Canada. This includes the outage time to complete the Change Request and any outage time required for back-out of the Change Request. Any outage that extends beyond the maintenance window approved in the original Change Request will be treated as the Service being unavailable and this outage period must be taken into account in the calculation of Service Level Target Service Availability (SLT-SA) and Service Level Target 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 maintenance window as outage time for the Service.

(93) If the execution of a Change Request causes an unplanned impact or outage to a Service, or it is determined that it will exceed the maintenance window approved by Canada, the Contractor must contact Canada immediately. The Contractor must provide a detailed explanation of the impacts and the plan to restore the Service or complete the Change Request as quickly as possible. The Contractor must also initiate an Incident Ticket for any outage not identified in the Change Request.

(94) Any outage to a Service that occurs as a result of an Emergency Change Request initiated by the Contractor will be treated as the Service being unavailable.

(95) The Contractor must escalate Change Requests based on the Change Request impact to Canada, and length of time that the Change Request has remained open, if requested by Canada. The Change Request escalation process will be determined after Contract award.

(96) A Change Request Ticket must include dedicated information fields for each Change Request as specified by Canada.

(97) The Contractor must automatically update a Change Request Ticket following a change in Work associated with the Change Request.

(98) The Contractor must back out a Change Request, using the back-out procedures specified in the Change Request Ticket, when the Change Request has caused a disruption to Services or the Change Request did not achieve the objectives of the Change Request.

(99) The Contractor must enter information in the Change Request Ticket log for a failed Change Request explaining the failure, and change its status to unsuccessful after completing the Change 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 Change Request and what partial changes were implemented.

(100) The Contractor must provide a Post-Change Request Report to Canada within 5 FGWDs of a failed Change Request.

8.4.2 Request Fulfillment

(101) The Contractor must use Change Management for all changes required for a Service Request.

(102) The Contractor must create 1 or more Service Request Tickets for each Service Request submitted by Canada.

(103) A Service Request Ticket must include the dedicated information fields as specified by Canada.

(104) The Contractor must update a Service Request Ticket following a change in Work associated with the Service Request.

(105) The Contractor must provide a Post-Service Request Report to Canada within 5 FGWDs of a failed Service Request.

(106) The Contractor must provide a base number of Service Requests in **Error! Reference source not found.** per calendar year in accordance with the following Service Request Levels:

a) To be completed for the requirement

(107) The Contractor must provide the following Service Catalogue Items for additional Service Requests as specified in a Service Order :

a) To be completed for the requirement

(108) Where Canada issues a Service Request that is not defined in Table 5 Canada will assign a Service Request Level as mutually agreed between SSC and the Contractor. Where there is no mutual agreement, the Service Request will be assigned a Service Request Level by SSC based on similar level of Work effort for other Service Requests. Unless otherwise specified in Table 5 and elsewhere in the Contract, Work for Configuration Management is not applicable to Service Requests.

Table 5. Service Requests

Service Request ID	SERVICE REQUEST DESCRIPTION	SERVICE REQUEST LEVEL
	To be completed for the requirement	

8.4.3 Release Management

(109) The Contractor must use Change Management for all changes required for a Service Release.

(110) The Contractor must develop and implement procedures for the distribution, installation, and rollback of changes for a Service Release.

(111) The Contractor must update all documentation following completion of a Service Release.

(112) The Contractor must implement Service Releases within 6 months of general commercial availability, when requested by Canada.

(113) The Contractor must implement Service Releases during maintenance windows approved by Canada.

(114) The Contractor must ensure that all changes for a Service Release are fully tested prior to being implemented.

(115) The Contractor must not use Services in production to test a Service Release prior to any changes.

(116) The Contractor must provide a Post-Service Release report to Canada within 5 FGWDs of a failed Service Release that includes a Service Release that:

a) had to be backed out;

b) that caused disruption to the Services for more than the maximum time of 2 hours, or

c) did not achieve the Contractor’s objective and therefore may need to be repeated at a later date.

8.4.4 Event and Incident Management

(117) The Contractor must proactively monitor Services for Incidents 7 days per week, 24 hours per day, 365 days per year.

(118) The Contractor must co-operatively work with Canada, Clients and any other third parties identified by Canada to resolve Incidents.

(119) The Contractor must open an Incident Ticket within 5 minutes of detecting an Incident or receiving a notice from Canada reporting an Incident.

(120) The Contractor must update the Incident Ticket log within 5 minutes of a change in status for any Incidents identified by Canada as high priority, and within 15 minutes of a change in status for all other Incidents.

(121) The Incident Ticket must include dedicated information fields specified by Canada for all Incidents.

(122) The Contractor must maintain a list of critical Applications, as specified by Canada, which are to be treated with the highest priority. Canada may identify an Application 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.

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

(124) The Contractor must assign the highest priority to Incidents for critical Applications.

(125) The Contractor must provide Canada with an operational escalation matrix and a management escalation matrix for Incidents that:

a) defines the primary contact for each level of escalation;

b) defines the alternates (of equal authority) for each level of escalation; and

c) contains clear instructions for contacting the primary and alternate escalation authority.

(126) The Contractor must notify Canada of Incidents according to the operational and management escalation matrices.

(127) The Contractor must categorize and assign Incidents with a priority level in accordance with a scale specified by Canada. Incident categorization and priority levels will be determined after Contract award.

(128) The Contractor must revise the priority of an Incident when requested to do so by Canada within 15 minutes of the request.

(129) The Contractor must automatically escalate Incidents according to priority and time periods specified by Canada.

(130) The Contractor must notify Canada of Incidents with priority levels specified by Canada, within 5 minutes of detection of the Incidents.

(131) The Contractor must provide an estimated time for resolution within the Incident Ticket.

(132) The Contractor must document in the Incident Ticket activity log all:

a) management and technical escalations for Incidents;

b) interactions with third parties; and

c) investigation, troubleshooting and analysis details, resolution activities and communications for Incidents.

(133) The Contractor must record in its Incident Ticket the date and time that each update is provided to Canada, and must record any direction Canada provides related to the frequency of updates, change in priority, and escalation, including the name of the Canada representative providing each direction.

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

(135) The outage time for an Incident must start at the time (start time) that the Incident is detected by the Contractor, or reported to the Contractor by Canada, whichever occurs first.

(136) The outage time for an Incident ends at the time that the affected Services are fully restored in relation to that Incident.

(137) The Contractor must request access to a Canada SDP when access is required to resolve an Incident.

(138) The Contractor must suspend outage time for an Incident at Canada’s request or where the Contractor has requested:

a) access to an SDP necessary to resolving an Incident, but Canada is unable to provide access; and

b) closure of an Incident Ticket pending Canada’s approval, but Canada is not available to consider the request.

(139) The Contractor must restart the outage time for an Incident at the point in time where the outage time has been suspended for an Incident when:

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

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

(140) Where outage time for an Incident was suspended and the Contractor was able to resolve the Incident without access to a Canada SDP (e.g. dispatch resource to the site), the Contractor must include the suspended outage time in the total outage time for the Incident.

(141) 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 must be documented with the adjusted outage time field within the Incident Ticket.

(142) The Contractor must review the outage time recorded for an Incident Ticket with Canada to ensure completeness of information and accuracy and obtain Canada's acceptance that the outage time is correct.

(143) The Contractor must update any and all affected reports within 1 FGWD 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.

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

(145) 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 or open a new Incident with a cross reference to the previous Incident, 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.

(146) The Contractor must review an Incident Ticket for completeness and accuracy within 1 FGWD 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 explain any adjusted outage time.

(147) 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.

(148) The Contractor must work with Canada to develop the outage time reconciliation process. The purpose of the process is to facilitate a joint review of Incidents and the measurement of outage times such that Canada 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 3 FGWDs of closing the Incident Ticket. The process must include Canada's online approval and acceptance of the outage times recorded in the Contractor's Incident Tickets.

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

(150) The Contractor must provide a briefing for an Incident within 1 FGWD of a request by Canada for an Incident. The briefing must be based on a format specified by Canada.

(151) The Contractor must provide a Post-Incident Report within 5 FGWDs of a request by Canada. If Canada finds the Post-Incident Report to be incomplete or inaccurate, it will advise the Contractor of the deficiency. Following such a notification, the Contractor must re-issue the report addressing the deficiency within 2 FGWDs. If Canada continues to find the Post-Incident Report deficient, it will be considered as not delivered and Canada will advise the Contractor accordingly.

(152) The Contractor must provide Canada with ongoing updates for the action plans contained within its Post-Incident Reports. The Contractor must notify Canada in advance when it becomes aware that it will not meet target dates specified in its action plans.

8.4.4.1 **Security Incidents**

(153) The Contractor must report any security breach as a Security Incident immediately (within 5 minutes) upon learning of its existence and create a Security Incident Ticket where security breaches can include but not limited to:

a) denial of service attacks;
b) unauthorized intrusion or access;
c) social engineering;
d) malware; or
e) information breach;
f) for unauthorized configuration changes; and
g) any suspected or actual privacy or security violation for Canada Data.

(154) The Contractor must report daily progress of Security Incidents to Canada, until each open Security Incident is fixed or mitigated.

(155) The Contractor must not withhold from Canada any information or data in its possession related to a Security Incident.

(156) Security Incident Tickets must include the following additional information:

a) detailed description of attack/event;
b) assessment of success of attack/event;
c) scope of the attack/event;
d) source/origin of attack/event;
e) estimated injury;
f) estimated impacts;
g) status of mitigations; and
h) applicable logs or evidence data.

(157) The Contractor must retain Security Incident Tickets throughout the Contract Period.

(158) The Contractor must provide evidence associated with a Security Incident, based upon criteria specified by Canada, within 72 hours, that includes results and analysis of logs and audit records research; and

(159) During a Security Incident, the Contractor must reduce the standard response time according to the priority of the Security Incident as specified by Canada.

(160) The Contractor must not include any classified or potentially harmful information, as determined by Canada, in Security Incident Tickets.

(161) The Contractor must separate information that identifies or details Security Incidents from all other types of Incidents.

(162) The Contractor must mitigate a security vulnerability identified in a Security Incident according to a mitigation plan approved by Canada as follows:

a) high-risk vulnerabilities within 10 FGWDs of Canada's approval of the mitigation plan; and
b) moderate risk vulnerabilities within 30 FGWDs days of Canada's approval of the mitigation plan.

(163) The Contractor must annually test the Security Incident Response Plan by:

a) documenting the test results; and
b) reviewing the test results with Canada within 10 FGWDs of completing the testing.

(164) The Contractor must update the Security Incident Response Plan within 20 FGWDs of completing the annual testing.

(165) 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 Canada's priority level assignments for Security Incidents.

8.4.5 Problem Management

(166) The Contractor must pro-actively identify, investigate, diagnose, analyze (trend) and correlate Incidents in order to determine Problems and Known Errors.

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

(168) The Contractor must designate network performance exceptions, where performance degradation has been identified by Canada as a Problem.

(169) The Contractor must create a Problem Ticket for each Problem.

(170) The Contractor must obtain Canada's approval to close a Problem Ticket.

(171) The Contractor must not suspend a Problem Ticket without Canada's approval.

(172) The Contractor must assign impact, urgency and priority to a Problem Ticket as specified by Canada.

(173) The Contractor must associate Incidents to existing or new Problems as requested by Canada.

(174) The Contractor must manage Problems through to resolution, ensuring that root cause is determined, preventive measures are implemented, and appropriate "clean-up" is done to remedy the Problem.

(175) A Problem Ticket must include dedicated information fields as specified by Canada for all Problem,:

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

(177) The Contractor must identify and investigate Known Errors until they are eliminated.

8.4.6 Configuration Management

(178) Configuration Management performed by the Contractor must include:

a) the configuration of Services;

b) the identification, configuration, tracking, programming and implementation of all Configuration Items (CIs), their attributes and their relationships to meet the on-going operational requirements of the ECCS in accordance with Canada's requirements; and

c) processes for:

i) determining the types of changes that are configuration controlled;

ii) approving configuration-controlled changes with explicit consideration for security impact analyses;

iii) documenting approved configuration-controlled changes;

iv) retaining and reviewing records of configuration-controlled changes; and

v) auditing activities associated with configuration-controlled changes.

(179) The Contractor must manage the configuration settings for ECCS by:

a) specifying component configuration settings to implement Operator least privilege/functionality;

b) documenting exceptions to configuration settings; and

c) monitoring, controlling and implementing changes to the configuration settings in accordance with Change Management, Request Fulfillment and Configuration Management processes.

(180) The Contractor must develop, document, and maintain the current baseline configuration of ECCS with traceability back to previous versions.

(181) The Contractor must audit all hardware and software default configuration settings against current baseline configuration for ECCS..

(182) The Contractor must ensure that only authorized Configuration Items are released and/or implemented.

(183) The Contractor must log each Configuration Item addition, removal or modification where each log entry in a configuration log file must include:

a) date and time of Configuration Item change; and

b) the unique User identifier of the resource making the change.

(184) The Contractor must provide Canada access to configuration log files for a rolling 3-year period using the Service Portal that allows Canada to:

a) view configuration log files based on a time and date specified by the User; and

b) download configuration log files using a file naming convention to be specified by Canada and using a COTS file format approved by Canada.

(185) The Contractor must archive configuration log data for the Contract Period and provide the archived configuration log data.

(186) The Contractor must maintain incremental daily back-ups of the configuration data of Services and Canada Data and store the 10 most recent copies of the daily backups at a location that is not co-located with the Services..

8.5 Service Portal

(187) The Contractor must provide Canada with a Service Portal, accessible by using a web browser 7 days per week, 24 hours per day and 365 days per year from the Internet.:

(188) The Contractor must use Release Management for Service Portal changes and for any changes to systems and services accessed by the Service Portal.

8.5.1 Registration and Access

(189) The Service Portal must allow a minimum of 50 concurrent Users and a minimum of 500 Service Portal Accounts.

(190) The Service Portal must provide User access as follows:

a) include a secure access connection (e.g. TLS 1.2);

b) minimize the requirement for logins;

c) request a unique User ID;

d) password credentials for Level 2 Assurance as described in ITSG-31;

e) enforce a idle session timeout period; and

f) deactivate the User account after a password is entered incorrectly after a number of times.

(191) The Service Portal must include password expiry and recovery for Service Portal Accounts using a process approved by Canada.

(192) The Service Portal must log the following transactions for Level 3 Assurance:

a) password changes;

b) credential registrations;

c) password recovery;

d) expired credentials;

e) authenticated User sessions; and

f) denied User sessions, including indication of from an invalid or inactive account.

(193) The Service Portal Accounts must include role-based access controls that define the rights (e/g/., read/view, write/modify, delete, download) that a User has when accessing Service Portal pages, applications, functions and data accessible on the Service Portal.

(194) The Service Portal must include a “least privilege policy” for all Service Portal Accounts, meaning:

a) the access control mechanisms must be configured to implement least privilege, allowing Users (and processes acting on their behalf) only to have access to those processes that are necessary to accomplish assigned tasks;

b) non-privileged Service Portal Accounts must be created for read-only access;

c) authorization to privileged Service Portal Accounts must be restricted to designated Service Portal Administrators; and

d) it allows the delegation of Service Portal Administrators and sub-delegation by existing Service Portal Administrators.

(195) The Service Portal must allow on-line self-registration of Users using a process approved by Canada.

(196) The Contractor must provide an electronic file of the Service Portal access log records for the previous 12 months to Canada, within 20 FGWDs of a request, using a file-naming convention and a COTS file format specified by Canada.

8.5.2 Administration

(197) The Service Portal must allow authorized Users to reset their password.

(198) The Service Portal must allow Canada administrators to manage Service Portal Accounts by:

a) creating, modifying, deleting, re-activating/de-activating Service Portal Accounts;

b) creating, modifying, and deleting Access Profiles;

c) authorizing self-registration requests for Users;

d) querying, sorting and viewing User profiles based on any field in a User profile; and

e) downloading query results with a file naming convention specified by Canada and COTS file format.

8.5.3 User Interface

(199) The Service Portal must be efficient and easy to use in the areas of presentation, organization, navigation, report generation and search tools.

(200) The Service Portal must allow a User to select the English or the French interface upon logon to the Service Portal, and toggle between the English and French interface after logon, that includes:

a) orientation and introduction pages with Contractor contact information as specified by Canada; and

b) online context-sensitive help function.

8.5.4 Document Management

(201) The Service Portal must provide document management that allows a User to:

a) download/upload a document with a file naming convention and COTS file format selected by the User;

b) search and sort for documents based on any date range, status (e.g., new, authorized, in progress, completed), or type;

c) open documents in the application in which they were created such as Microsoft Word; and

d) print documents.

8.5.5 Report Management

(202) The Service Portal must allow a User to:

a) access reports over the entire Contract Period by searching and sorting based on on any field (and multiple fields) and date range;

b) create and view real time reports by selecting:

i) available data sources;

ii) date and time ranges;
iii) criteria for the selected fields; and
iv) tabular or graphical format where applicable;
v) fields to appear on the report.

c) search, sort, and view reports based;
d) save a real time report as a document with a file name and in COTS format selected by Canada (PDF, Word, Excel);
e) download reports with a file name and COTS format selected by the User, where the COTS format can include:
i) Microsoft Excel (MS Excel) for numerical reports with predefined headers and formatting as approved by Canada;
ii) CSV for numerical reports;
iii) HTML;
iv) PDF; and
v) Microsoft Word (MS Word).

8.5.6 Information Management

(203) The Contractor must allow a User to download Service Portal Data selected by the User using a file-naming convention and a COTS file format specified by Canada

(204) The Contractor must obtain the written consent of the Technical Authority before deleting any Service Portal Data from the Service Portal.

(205) The Contractor must implement back-up and recovery for Service Portal Data by:
a) making daily back-ups; and
b) making and storing a weekly back-up of Service Portal Data off site.

8.6 Security and Privacy

8.6.1 Ongoing Security Assessment

(206) On an annual basis, the Contractor must provide:
a) a SOC2 Type 2 report; and/or
b) evidence that demonstrates current certification for ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements.

8.6.2 Plan of Actions and Milestones

(207) The Contractor must provide a Plan of Actions and Milestones for Canada's approval within 20 FGWDS of a request from Canada that:
a) documents the remedial actions planned by the Contractor to correct Vulnerabilities and security deficiencies identified during the Security Assessment and in any subsequent SOC2 Type II report or ISO re-certification; and
b) includes a Project Schedule to complete the remedial actions; and

(208) The Contractor must update the Plan of Actions and Milestones based on the results from security assessments, security impact analyses, and security monitoring activities conducted by the Contractor.

(209) The Contractor must implement the remedial actions identified in the Plan of Actions and Milestones in accordance with the Project Schedule for the initial approved version and any subsequent versions.

8.6.3 Service Contingency Plan

(210) The Contractor must ensure that the Service Contingency Plan is:

a) coordinated with organizational elements responsible for related plans including incident handling teams;

b) communicated and distributed to organizational elements involved with executing the plan; and

c) protected from unauthorized disclosure and modification.

(211) The Contractor must notify Canada immediately upon determining that a disaster or other emergency situation has occurred that affects Services. The notification must include the following information: a brief description, date/time, estimated restore time, and impacted SDPs.

(212) The Contractor must test Service Contingency Plan (all processes, procedures, roles, responsibilities etc.) annually as documented in the approved plan, and provide the test results to Canada within 20 FGWDs of completing the testing.

(213) The Contractor must restore Service functions as part of Service Contingency Plan testing. The restoration exercise must not be performed using production Services unless otherwise approved by Canada.

(214) The Contractor must correct any problems to Services identified during the testing of Service Contingency Plan within 60 FGWDs after completion of the testing.

(215) The Contractor must provide to Canada within 40 FGWDs of a Service Request, evidence not more than 12 months old (e.g., test results, evaluations, and audits, etc.) that Service Contingency Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Service Contingency requirements for Services.

8.6.4 Privacy Management Plan

(216) The Contractor must review the Privacy Management Plan annually and provide a report to Canada within 20 FGWDs of completing the review that summarizes the results of the review and proposed changes. The Contractor must update the Privacy Management Plan within 20 FGWDs of Canada's acceptance of the report.

(217) The Contractor must provide to Canada within 40 FGWDs of a request, evidence not more than 24 months old (e.g., test results, evaluations, and audits) that the Privacy Management Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Canada's privacy management requirements.

8.6.5 Vulnerability Management

(218) The Contractor must run automated vulnerability assessment testing against all ECCS infrastructure components on a monthly basis, or as specified by Canada.

(219) The Contractor must allow Canada, or its representatives to conduct vulnerability assessment testing, limited to discovery and scanning activities of ECCS infrastructure and excluding any disruptive or destructive activities, on an annual basis against ECCS within three (3) FGWDs of a request by Canada, that includes:

a) physical access to the ECCS facilities (i.e. Contractor's facilities where the ECCS infrastructure is located);

b) network access(es) to the ECCS infrastructure to allow for authenticated and unauthenticated scanning of network components and security appliances, using Canada operated equipment, and Canada specified tools. ; and

c) assistance for the duration of any onsite portion of the vulnerability assessment of at least one technical resource that is familiar with the technical aspects of the ECCS infrastructure (i.e., the hardware, software, and network components, security appliances, and their configuration).

(220) The Contractor must provide a Vulnerability Assessment Report Plan for Canada's approval within 20 FGWDS of a request from Canada based on the Vulnerability Assessment Plan developed for Service Readiness that includes:

a) a listing of the vulnerability assessment tests that were conducted; and

b) for each vulnerability assessment test case:

i) whether a known vulnerability was detected;

ii) a description of the vulnerability;

iii) a description of the patch or corrective measure that was implemented to resolve the vulnerability; and

(221) c) for any unresolved vulnerability:

i) an assessment of the significance of the vulnerability in the context of ECCS;

ii) the problem ticket number for the outstanding patch or corrective measure; or

iii) the rationale for not implementing a patch or a corrective measure.

(222) The Contractor must provide a Vulnerability Mitigation Plan within five (5) FGWDs of completion of a vulnerability assessment where security deficiencies are identified that includes proposed protection measures to mitigate the risks identified from the vulnerability assessment testing.

(223) The Contractor must produce a Vulnerability Mitigation Report after completion of remediation activities completed for a Vulnerability Mitigation Plan that includes:

a) a description of the corrective measures implemented; and

b) proof that associated system documentation has been updated to reflect the changes.

(224) The Contractor must mitigate all security deficiencies found in accordance with Canada's security requirements at no additional cost to Canada as a result of vulnerability testing by the Contractor and Canada.

8.6.6 Patch Management

(225) The Contractor must provide patch management for the ECCS infrastructure components that includes:

a) ensuring the latest version of applications and operating systems are used;

b) ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a

c) timely manner;

d) prioritizing critical patches using a risk-based approach;

e) taking applications offline and bringing them back online;

f) aligning criticality levels for patches as specified by Canada;

g) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v3; and

h) testing and verification methodology to ensure that patches have been implemented properly.

8.7 Service Engineering and Design

(226) The Contractor must initiate a Service Request for changes to the Service Design as requested by Canada that includes a description of any Service Design options reviewed and any record of decisions in the Service Request log.

(227) The Contractor must engineer and design the ECCS requested by Canada in Service Orders that includes:

a) integration with Services specified by Canada;

b) evaluating Canada's technical, functional, and operational requirements;

c) reviewing and analyzing Key Performance Indicators and Service Levels Targets;

d) adapting, tuning, and improving Services to ensure optimal performance; and

e) proactively assessing the capacity for Services and providing recommendations for capacity changes.

8.8 Reports and Documents

(228) The Contractor must define the content and format of reports:

a) in consultation with Canada and subject to Canada's acceptance;

b) in a manner that does not require Canada to reformat them in order to make them more usable or presentable;

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

d) that allow Canada to generate reports efficiently. This includes 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;

e) to be efficient to view 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 so 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.

(229) It is Canada's intention to use existing reports provided by the Contractor where possible as solely determined by Canada. The exact reports will be determined during consultation with Canada before the completion of Service Readiness.

(230) The Contractor must provide reports in English using the ET time zone.

(231) Information in reports representing numbers and dates must be downloadable as numbers and dates, and not formatted as text.

(232) The Contractor must provide all annual reports within 30 FGWDs of the end of the previous 12 months, based on the anniversary of the Contract.

(233) The Contractor must provide all weekly reports within 2 FGWDs of the end of the previous week where the end of a week is 11:59 pm Friday.

(234) The Contractor must provide all monthly reports within 5 FGWDs of the end of the previous month where the end of a month is 11:59 pm on the last FGWD of the month.

(235) The Contractor must provide Canada with all reports provided to other clients of the Contractor for Services using Canada Data

(236) The Contractor must not make any structural changes (format, content provided) to an approved report without following the Request Fulfillment processes.

(237) The Contractor must develop and maintain on an ongoing basis a Data Dictionary for all reports that must include:

a) definition of each data element (name, size, type, filed length, etc.);

b) wireframe view;

c) how each report is to be accessed on the Service Portal;

d) detailed description of measurement methodology for each data element of the report including:

i) data collection (what data, where the data is collected and how);

ii) data aggregation;

iii) data calculations; and

iv) data sampling (size, frequency, interval, duration etc.).

(238) The Contractor must provide, within 5 FGWDs of a written request by Canada, the following ECCS documentation:

a) call flow diagrams (in Visio format);

b) Service Applications and business rules;

c) PSTN provisioning records (including local and Toll Free telephone numbers);
d) recorded announcements;
e) Real-Time and Historical Reports; and
f) physical and logical connectivity of all ECCS components, including topologies and IP addresses allocation in Visio format.

(239) The Contractor must provide the Service Operations reports summarized in Table 6 according to frequency, purpose, and description.

Table 6. Service Operations Reports

Report Name	Service Management Summary Report
Frequency	Scheduled, Monthly
Purpose	The report must present a summary of the Contractor's performance in delivering the services and meeting Service Level Targets (SLTs).
Description	The report must include: a) total number of Incidents and the total number of SLT exceptions for the monthly period; b) list of all Incidents for the monthly period organized by type, priority, and SLT, identifying Incident Ticket numbers and escalation levels invoked; c) list of SLT exceptions for the monthly period identifying the SLT for each exception and the amount by which the SLT was missed (applies to all types of SLT exceptions whether or not there is an associated Incident Ticket); d) description of the recommendations, corrective actions and timeframes to implement any required changes to resolve chronic Problems or service degradation and/or prevent future SLT exceptions; e) description of Incidents and issues related to the Contractor's services such as the Service Portal and its associated systems, tools and applications (e.g., CMDB, reporting, etc.), including the corrective actions and timeframes to resolve them; f) Service Requests completed/pending; g) Change Requests completed/pending
Report Name	Service Request and Change Request Report
Frequency	Scheduled, Monthly
Purpose	The report must present a detailed summary of all Service Requests planned or completed during the reporting period.
	The report must include: a) Service Requests closed for the weekly period b) Service Requests pending execution c) Change Requests closed for the weekly period, including the following:

	d) Change Requests pending execution, including the following:
Report Name	Post-Incident Report
Frequency	On-Demand, Within 2 FGWDs of Canada's request
Purpose	This report must provide Canada with an in-depth understanding of any Incident that Canada considers to have had a significant impact on its business. The report must clarify exactly what occurred during the Incident, including the Contractor's actions, as well as the Contractor's plans to address any potential recurrence.
Report Name	Post-Change Request Report
Frequency	On-Demand. The FGWD immediately following the execution of any Emergency Change Request and/or within 5 FGWDs of a failed Change Request or Service Release
Purpose	The report must provide Canada with an in-depth understanding of a failed Change Request, or an Emergency Change Request.
Report Name	Post-Service Request Report
Frequency	On-Demand, The FGWD immediately following the execution of any Emergency Service Request and/or within 5 FGWDs of a failed Service Request
Purpose	The report must provide Canada with an in-depth understanding of a failed Service Request, or an Emergency Service Request.
Report Name	Service Release Summary Report
Frequency	Scheduled, Monthly
Purpose	Summary of Service Release Activity
Description	The report must include, for each Service Release in the preceding month: a) time and date of the Service Release; b) purpose of the Service Release; c) description of Service Release activities; d) Enterprise Contact Centre Services components affected; and e) lessons learned (if Service Release failed).
Report Name	Planning and Engineering Report
Frequency	Scheduled, Annually
Purpose	The report is used by the Contractor and Canada to conduct a joint planning exercise for the coming year.

Description	The report must include the following, which covers the next 12-month period: a) impact of new requirements on the Enterprise Contact Centre Services; b) engineering and planning activities; c) plan for Service Releases; d) capacity baselines and trends; e) recommendations on technology innovation and improvements; f) recommendations for maintaining, improving and optimizing Enterprise Contact Centre Services; and g) recommendations for a PO1 Grade of Service for PSTN Service by Application.
Report Name	Service Ticket Report
Frequency	Real time, as required.
Purpose	A User-definable report that must provide access to Incident Tickets, Problem Tickets, Change Request Tickets and Service Request Tickets based on ticket type selected by Canada and any ticket field over a time period selected by the User..
Description	The report generator must provide: a) ability to search, sort and view tickets; b) ability to download ticket query results using a file naming convention specified by Canada and COTS file format; c) ability to view individual tickets (all fields) in a hierarchical tree fashion where information within a ticket can be viewed in a successive “drill-down” manner (i.e., related tickets) by selecting hyperlinks; d) cumulative report detailing for each ticket in the query results: the ticket number, date, priority, associated tickets (where applicable), impacted Enterprise Contact Centre Services, outage time, detailed description of ticket; e) direct access to the CIs from the CMDB involved by selecting a hyperlink in the ticket; and f) ability to generate open or closed ticket summary information, displayed in graphical and tabular format, by year, month, day and hour intervals for number of tickets, and number of tickets by priority level.
Report Name	Privacy Summary Report
Purpose	Personal information that is collected, used, disclosed, retained or disposed of as part of Services
Frequency	Within 30 calendar days of the end of each quarter (January-March; April-June; July-September; October-December)
Description	The report must include the following information: a) a description of any new measures taken by the Contractor to protect the Personal Information (e.g. new software or access controls being used by the Contractor);

	b) a description of any changes made to the software, the access controls and the operating procedures, which may have privacy implications; c) a list of any corrections made to Personal Information at the request of Canada on behalf of an individual (including the name of the individual, the date of the request, and the correction made); d) details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the Contractor; e) a list with details of any privacy breaches; and a complete copy (attached annex to the report, in a file format specified by Canada) of all the Personal Information stored electronically by the Contractor.
Report Name	Personal Information Report
Purpose	This report must provide a summary of activities for Personal Information
Frequency	Quarterly
Description	The report must include: a) description of any new measures taken by the Contractor to protect the Personal Information (eg. new software or access controls being used by the Contractor); b) description of any changes made to the software, the access controls and the operating procedures, which may have privacy implications; c) list of any corrections made to Personal Information at the request of Canada on behalf of an individual (including the name of the individual, the date of the request, and the correction made); d) details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the Contractor; and details of any privacy breaches of Personal Information.

8.9 Training

(240) When requested by Canada in Service Orders, the Contractor must provide virtual classroom training for the Service Catalogue Items (SCIs) in Table 7 in accordance with the Training Module.

Table 7. Service Catalogue Items for Training Sessions

SCI	Training Module
SCID:VC-Training-ITSM	Service Management
SCID:VC-Training-Portal	Service Portal
SCID:VC-Training-Agent	Agent
SCID:VC-Training-Team Leader	Team Leader
SCID:VC-Training-Reports	ECCS Reports
SCID:VC-Training-Admin	Administrator

(241) The Contractor must provide Training Sessions in English and French, as specified by Canada.

(242) The Contractor must provide the instructor for the Training sessions.

(243) The Contractor must provide a Training during the hours of 9 am to 5 pm ET on FGWDs for a Training Session that allows:

a) up to 50 concurrent participants (based on the number that Canada enrolls);

b) each participant to view the Training Module content as it is presented by the instructor; and

c) each participant to have audio interaction with the instructor.

8.10 Service Level Targets

(244) The Contractor must design, implement, manage and operate the Services so that they meet the Service Level Targets (SLTs) defined in this section.

(245) The Contractor must monitor, measure, calculate, and report on SLTs 7 days per week, 24 hours per day, 365 days per year, unless otherwise indicated for a specific SLT.

(246) The Contractor must count omitted measurements as failed measurements, with the exception of measurements for Services that have an outage for which SLT-SA applies.

(247) The Contractor must commence Service Level Target and performance reporting for a Service immediately after the acceptance of the Work for a Service Order by Canada.

8.10.1 Outage Time

(248) Outage time for a Service begins from the time (start time) that the Incident is detected by the Contractor, or reported to the Contractor by Canada, whichever occurs first. The outage time used in the calculations ends when the affected Service is fully restored for the Incident.

(249) The Contractor's lack of proper security clearance (for itself or its personnel) does not excuse it from its obligation to restore the affected Service within the SLT.

(250) In cases where Canada attempts to report an Incident for an outage but the Contractor’s Service Desk does not answer the call, the start time for the outage begins at the time Canada placed the call to the Service Desk.

(251) The following events may, with Canada’s approval, be excluded from the calculation of outage time for a Service during a review of the Incidents associated with the outage:

a) failure related to a Security Incident where Canada has approved mitigation actions that impact the availability of ECCS;

b) loss of power at a Canada SDP beyond the time period for power backup provided by the Contractor;

c) an approved Emergency Service Request, which does not exceed a 2-hour period;

d) failure of another Service;

e) failure of Contractor Equipment resulting from damage caused by a party other than the Contractor or from the removal, relocation or tampering of the Contractor Equipment by a party other than Contractor;

f) scheduled downtime;

g) failure of a Canada Service, including data received from the Canada Service;

h) suspension of Incident Ticket;

i) Change Requests approved by Canada; or

j) Canada Service does not provide sufficient capacity.

8.10.2 Service Level Target for Service Availability

(252) The Service Level Target Service Availability (SLT-SA) must be greater than or equal to the following:

a) 99.999% where SLT-SA1 applies;
b) 99.990% where SLT-SA2 applies;
c) 99.900% where SLT-SA3 applies;

(253) The period of measure for SLT-SA is a calendar month (7/24); therefore the total number of minutes in the measurement period will vary based on the number of calendar days in the month.

(254) The Contractor must calculate SLT-SA as follows: ((measurement period – sum of the outage times) / measurement period) x 100.

(255) Example: measurement period: June = 30 days = 30 x 24 hours x 60 minutes = 43,200 minutes. Sum of all outage minutes for the SAP in the month: 98 minutes (excludes time associated with SLT-MTRS exception Calculation of SLT-SA: ((43,200 - 98) / 43,200) x 100 = 99.77%.

(256) The outage time for Incidents where a Service does not function in accordance with the Service Design must be included in the calculation of the SLT-SA for that Service.

(257) The outage time for any of the Incidents defined in ECCS Annexes must be included in the calculation of the SLT-SA for the Service.

(258) The outage times used in the calculation of SLT-SA exclude the outage times associated with SLT-MTRS exceptions. For example, if the outage for a Service with an SLT-MTRS4 is 4.5 hours, that outage time (4.5 hours) is not included in the sum of outage times used in the calculation of SLT-SA for the SAP.

8.10.3 Service Level Target for Maximum Time to Restore Service

(259) The Service Level Target Maximum Time to Restore Service (SLT-MTRS) must not exceed:

a) 15.0 minutes where SLT-MTRS0:15 applies;
b) 30.0 minutes where SLT-MTRS0:30 applies;
c) 1.0 hour where SLT-MTRS1 applies;
d) 2.0 hours where SLT-MTRS2 applies;
e) 4.0 hours where SLT-MTRS4 applies;
f) 6.0 hours where SLT-MTRS6 applies;
g) 8.0 hours where SLT-MTRS8 applies;
h) 12.0 hours where SLT-MTRS12 applies; ands
i) 24.0 hours where SLT-MTRS24 applies.

(260) The Contractor must measure SLT-MTRS on a per-Incident basis.

(261) The outage time associated with an SLT-MTRS exception must be excluded from the calculation of SLT-SA for the same Service. However, it is possible that both an SLT-SA and SLT-MTRS exception occur for the same Service in the same month. It is possible that even with the exclusion of the outage time associated with an SLT-MTRS exception; the sum of other outage times for the same Service also results in an SLT-SA exception for that Service.

(262) The outage times used in determining whether the SLT-MTRS has been met for a Service include the types of Incidents for which SLT-SA is calculated (refer to **Error! Reference source not found.**).

8.10.4 Service Level Target for Service Portal Availability

(263) The Service Level Target for Service Portal Availability (SLT-SPA) must be greater than or equal to 99.700% for User access any Service Portal function.

(264) The period of measure for SLT-SPA is monthly.

(265) The Contractor must calculate the availability as follows:

((measurement period – sum of the outage times) / measurement period) x 100

(266) The outage time used in the calculation of SLT-SPA begins from the time (start time) that User access is prevented to a Service Portal function, as and when detected by the Contractor or as and when reported to the Contractor by Canada, whichever occurs first. The outage time used in the calculation ends when Canada's access to the Service Portal function is fully restored, as and when confirmed by Canada.

(267) The outage time associated with the calculation of SLT-SPMTR must be excluded from the calculation of SLT-SPA for the same Service Portal function. However, it is possible that both an SLT-SPMTR and SLT-SPA outage occurs for the same Service Portal function in the same month. It is possible that even with the exclusion of the service outage time associated with an SLT-SPMTR exception, the sum of other service outage times for the same Service Portal function also results in an SLT-SPA exception.

8.10.5 Service Level Target for Service Portal Maximum Time to Restore

(268) The Service Level Target for Service Portal Maximum Time to Restore is less than or equal to 4 hours from the start of any Incident where the User is unable to access to any Service Portal function.

(269) The outage time used in the calculation of SLT-SPMTR begins from the time (start time) that the Incident for the Service Portal is detected by the Contractor, or is reported to the Contractor by Canada, whichever occurs first. The outage time used in the calculation ends when Canada's access to the Contractor's Service Portal functions is fully restored, as and when confirmed by Canada.

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

8.10.6 Service Level Target for Service Desk Response

(271) The Service Level Target for Service Desk Response (SLT-SDR) is that the Contractor’s Service Desk must answer 80.0% of all telephone calls placed by Canada within 20 seconds. The period of measure for SLT-SDR is the calendar month.

(272) The SLT-SDR must be calculated as follows:

(273) ((number of calls answered within 20.0 seconds + number of calls abandoned within 20.0 seconds) / (total number of calls answered + total number of abandoned calls)) x 100

(274) 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

(275) Service Desk agent, a live person, answers the caller. Although the Contractor may use voice scripts and menu options acceptable to Canada, the calculation of time to answer a call excludes any time spent by callers listening to and making menu selections in the Contractor’s Interactive Voice Response system prior to waiting in queue for the Contractor’s Service Desk agent. An abandoned call to the Service Desk is a call that is connected to the Contractor’s telephone system but that the Calling Party terminates before a Service Desk agent answers the call.

8.10.7 Service Level Target for Service Request Response

(276) The Service Level Target for Service Requests (SLT-SRRES) must be less than or equal to the Service Delivery Interval (SDI) as defined in Table 8, as the time for the Contractor to complete the Work associated with Service Requests.

(277) The SLT-SRES is measured on a per-Service Request basis.

Table 8. Service Level Targets for Service Requests

ITEM	SERVICE REQUEST DESCRIPTION	SERVICE REQUEST LEVEL	SDI

	To be completed for the requirements		

8.10.8 Service Level Target for Service Provisioning

(278) The Service Level Target for Service Provisioning (SLT-SP) must be less than or equal to the Service Delivery Interval (SDI) that is defined in Table 9 as the time for the Contractor to complete the Work associated with a Service Order.

Table 9. Service Level Targets for Service Provisioning

ITEM	SERVICE PROVISIONING DESCRIPTION	SDI
	To be completed for the requirements	

(279) The Contractor must calculate the time to complete the Work for SLT-SP as the number of FGWDs from the date of issuance of the Service Order to the Contractor, to the date that Canada accepts the Work.

8.10.9 Service Level Targets for Contractor Responsibilities

(280) With respect to the Service Level Targets for Contractor Responsibilities (SLT-CONRES), the actual time to perform the Work must be less than or equal to the Service Delivery Interval (SDI) that is defined in Table 10 as the time for the Contractor to complete that Work.

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

Table 10. Service Level Targets for Contractor Responsibilities

ITEM	CONTRACTOR RESPONSIBILITY DESCRIPTION	SDI
	To be completed for the requirements	

9 INSTALLATION

(282) There is no requirement for Canada to issue any Service Order for Installation Services for Work to be completed by the Contractor elsewhere in the Contract, with the exception for the Work identified in this subsection where Canada issues Service Orders for Installation Services.

(283) When requested by Canada in a Service Order, the Contractor must provide the Installation Services for the Service Catalogue Items (SCIs) in Table 11 in accordance with the Working Hours and Unit of Installation.

Table 11. Service Catalogue Items for Installation Services

SCI	Installation Service	Working Hours	Unit of Installation
SCID:Install-Recording-01	Recording English and French voice prompts	Core	Hourly rate
SCID:Install-Recording-02	Recording English and French voice prompts	Non-Core	Hourly rate
SCID:Install-Recording-03	Recording Other Language voice prompts (i.e. not French or English)	Core	Hourly rate
SCID:Install-Recording-04	Recording Other Language voice prompts (i.e. not French or English)	Non-Core	Hourly rate

9.1 Recording Voice Prompts

(284) The Work for SCID:Recording-01 and SCID:Recording-02 may include:

a) providing English and/or French recorded samples of Voice Talent for approval by Canada;

b) recording voice prompts provided by the Contractor and approved by Canada, or provided by Canada in English and/or French as specified by Canada;

c) documenting the purpose of the recorded voice prompts; and

d) storing the recorded voice prompts on the Service Portal.

(285) The Work for SCID:Recording-03 and SCID:Recording-04 may include:

a) providing recorded samples of Voice Talent for approval by Canada in the language specified by Canada;

b) recording voice prompts provided by the Contractor and approved by Canada, or provided by Canada as specified by Canada, in the language(s) specified by Canada;

c) documenting the purpose of the recorded voice prompts; and

d) storing the recorded voice prompts on the Service Portal.