Annex A

Canada Border Services Agency

Data Warehouse (DW) FOUNDATION
Data Management & Data Warehouse

STATEMENT OF REQUIREMENTS

TABLE OF CONTENTS

1.0 Introduction

1.1 Background

The Government of Canada created Shared Services Canada (SSC) on August 4, 2011, to fundamentally transform how the Government manages its information technology (IT) infrastructure. SSC reports to Parliament through the Minister of Public Works and Government Services Canada and is mandated to deliver email, data centre and telecommunication services to 43 federal departments and agencies. The creation of Shared Services Canada will improve the efficiency, reliability and security of the Government's IT infrastructure. A more efficient use of technology will increase productivity across departments and will help build a more modern public service. A priority of SSC is to maintain and improve the delivery of IT-infrastructure services while renewing the Government's aging IT infrastructure to adopt enterprise-wide approaches for managing IT infrastructure services and implement efficient and effective business management processes in support of our mandate.

One of the key deliverables of the CBSA eManifest major project launched in 2006 is the implementation of a Data Warehouse solution (DW). The mandate of eManifest it to strengthen the nation's security while modernizing and improving commercial border processes. Through the risk assessment of electronic pre-arrival data, the ability to target, screen, and detect patterns and trends will increase thereby enhancing the overall ability to identify and interdict potentially high-risk shipments while expediting the processing of low risk shipments. A Data Warehouse will support and facilitate these national requirements and be a foundation for many future major projects undertaken by the Canada Border Services Agency (CBSA), including Beyond the Border.

The current data warehouse infrastructure that is in place at CBSA cannot meet the performance and capacity capabilities requirements of this project. This procurement initiative is twofold. Firstly, to address the current infrastructure deficiencies as stated above, and secondly to address the issue that the existing DW foundation is aging technology and will soon reach its' technological "end-of-life". Given the current market place for this type of technology, an expansion of the existing DW foundation comes at a much higher cost than the acquisition of new technology. As well, it would be a short term solution based on dated technology that does not perform to the level of today's products with significant technology advances.

1.2 Future Environment

CBSA will focus on the latest technology in the data warehousing marketplace, which has great performance increases due to technology advances, is available at a much lower initial cost and is quickly and easily scalable to add capacity on demand.

Recent technology advances in Data Warehouse Foundation solutions have seen suppliers expand their offerings as complete functioning systems to include complete Data Warehouse solutions through development and acquisition activities. This allows single suppliers to supply and support entire Data Warehouse Foundation solutions. In addition, performance and capacity have grown exponentially with the new technologies and the single vendor integration of multiple technology options within their single product line to meet project/client requirements.

Canada is now moving to implement a demanding new application for Data Warehousing (eManifest) and to do so will require flexible Data Warehouse foundation options from the Contractor, who must meet the changing requirements over time, give a high level of performance and availability, include Disaster Recovery capability at a separate location, and maintained by a single responsible entity.

1.3 The Requirement

Canada has a firm requirement for a commercial off-the-shelf (COTS) technology hereafter referred to as the Solution. The required solution would be a single COTS based solution that is pre-integrated with all

necessary hardware, software, firmware, networking and storage, and is typically engineered to support high performance and high availability data warehouse environments. This solution would be the foundation infrastructure for CBSA's data warehouse that will be accessed by existing CBSA front-end client toolsets. This solution will ensure the capability to support the CBSA eManifest crown project deliverables for data warehouse & business intelligence. This solution will be required to support 5 separate environment requirements that CBSA has including Sandbox, Development & Testing, Pre-Production, Production as well as a Remote Disaster Recovery production environment.

The requirement includes options to provide for additional scaling capability to enhance both capacity and performance at each environment at each location, integration services, training, and related maintenance and support services.

The initial implementation of the new Data Warehouse Foundation (DWF) technology solution will be an "add-on" to Canada's existing DWF infrastructure. Various testing and integration services will be performed by Canada personnel with Contractor support as the project moves through the installation, integration and migration processes.

To ensure that full compliancy and operational effectiveness exists within the CBSA infrastructure, the Contractor's commercially available technology solution must be made available for Proof of Proposal testing. Business Intelligence software and enterprise data warehouse management software tools currently utilized and identified in Appendix 1 of this Statement of Requirement will continue to be used.

2.0 Business Requirements

The ever-growing costs of storage and hardware and the increased focus on performance ability due to extremely large data volumes, resulted in Canada exploring emerging technologies that will meet the eManifest Data Warehouse and business intelligence requirements as well as enabling scaling to meet Canada's future initiatives including Beyond the Border.

Obtaining this solution will provide Canada with the capability to support their clients in the CBSA e-Manifest initiative.. The integrated collection of internal and external data in the proposed data warehouse solution will be engineered specifically to include the performance and flexibility needed to satisfy complex queries across the large amounts of data required for optimal risk assessment.

Currently, long query times are impacting end user productivity and satisfaction and are also driving additional unnecessary CPU utilization which contributes additional cost to the overall environment. The solution must support transparency to end user applications with no requirement for changes to the end user applications. It must also maintain full availability and security of the data.

The solution consists of a Primary site and a Disaster Recovery site at two separate locations within the National Capital region.

The underlying business requirements that this solution is intended to address are as follows:

Provide a solution that together with existing front end consumption level tools, enables end users to:

a. Optimize the risk assessment of Commercial shipments prior to their arrival in Canada;
b. Improve the ability to actively monitor and target shipment activity resulting in enhanced security;
c. Support continuous improvement of business processes, data and technology related to the Commercial Border Management Program;
d. Support the business in its ability to visualize patterns and trends, to conduct ad hoc what-if analysis and simulate the business impact of emerging methods;
e. Empower and enable CBSA knowledge workers and analysts to proactively identify emerging threats, detect patterns and trends, and identify opportunities for improvement;

f. Improve the ability to assess and measure the effectiveness of the Border program on an on-going basis;
g. Support operational and informational business functions related to Commercial Border Management;
h. Provide the effective delivery of information to the “right” person (efficiency), in the “right” place (access), at the “right” time (timeliness), with the “right” level of detail (granularity) and the “right” level of quality (accuracy, completeness, validity)to enhance the decision making process.

The functional requirements of the intended solution are as follows:

1. An availability of 99.95% over a 24/7/365 annual term must be provided;
2. Total current data requirements are not to exceed 200TB but could be increased at Canada’s discretion;
3. The solution must provide isolation between Sandbox, Development/Test, Pre-Production and Production environments such that the workload, modifications or outage in one environment cannot impact another environment; furthermore, the Production and Disaster Recovery environments must be physically isolated but interconnected with other environments;
4. In the case of an un-scheduled downtime from a damaged solution component the Recovery Time Objectives(RTO) are as follows:
    - Data Warehouse - 24 Hours;
    - Standard Data Mart - 24 Hours;
    - Critical Data Mart - 4 hours;
5. In case of disaster or elongated outage at the primary site causing users to lose connectivity and have to sign in again and/or cause current transactions to be interrupted:
    - Disaster Recovery site must provide service for the “critical” data marts;
6. Data warehouse and non-critical Marts will be rebuilt by Canada from backups;
7. Current existing timeframes for production performance must be improved considerably through the acquisition of a new solution technology; and
8. Solution must function with current BI consumption layer.

3.0 Technical Requirements

3.1 General Requirements

Because the Data Warehouse marketplace is a rapidly changing environment with the advent of technology advances and corporate acquisitions, the Contractor must upgrade the Solution as components are upgraded and released to the market at no additional cost to Canada during the life of the Contract.

3.1.1	The Contractor must certify that the Solution is Appliance based and complies with the definition of a “COTS System” as defined in Appendix 3 of the SOR.
3.1.2	The Contractor’s Solution must be comprised of components which are the latest version released by the OEM and Generally Available.
3.1.3	The Contractor’s Solution must be rack mountable or self-standing.
3.1.4	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.1.5	The Contractor must identify the number of licences that would be included as part of their Solution, for both the baseline requirement and scaled versions of the Solution for the Primary and Disaster Recovery locations as identified.
3.1.6	The Contractor's Solution must have a constant availability of 99.95%.
3.1.7	The Contractor's Solution must be capable of loading a minimum of 2 TB in 1 hour.
3.1.8	The Contractor must agree that all technology aspects of their Solution as included under the Contract are to be replaced by latest available technology from the Contractor as released for sale in the marketplace at no additional cost to Canada during the life of the Contract and any extensions issued thereto.
3.1.9	The Contractor must deliver, install, and maintain the Solution at a separate primary location and a Disaster Recovery location in the National Capital Region.
3.1.10	The Contractor's Solution must store objects consisting of up to a minimum of 2 Gigabytes per object of image, audio and video data.
3.1.11	The Contractor's Solution must permit a minimum of 16 tables in a single query join.
3.1.12	The Contractor's Solution must support English and Canadian French character sets.
3.1.13	The Contractor's Solution must include a data extract capability which will spawn multiple concurrent processes to unload records from a table without preventing queries on that table.
3.1.14	The Contractor must include on-site support during the installation and integration of the Solution at both Primary and Disaster Recovery sites.
3.1.15	The Contractor must include a detailed delivery, integration and acceptance schedule as approved by the Technical Authority.
3.1.16	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.1.17	The Solution must provide isolation between Sandbox, Development/Test, Pre-Production and Production environments such that the workload, modifications or outage in one environment cannot impact another environment; furthermore, the Production and Disaster Recovery environments must be physically isolated from other environments. a. Sandbox b. Development/Test c. Pre-Production d. Production e. Disaster Recovery Production
3.1.18	The Contractor's Solution must not degrade Query response times by more than 10% when tables being queried begin receiving updates regardless of data size.

3.2 Baseline Requirement

3.2.1 Baseline Capability

The Contractor must provide a baseline Solution that is + or – 10% of the usable storage capacities for each of the separate environments as shown in the Table below. The Solution shall include all hardware, software, licenses, integration services and connectivity between the Primary and Disaster Recovery sites.

Table 1 shows the baseline capacity requirements and the number of concurrent users in various raw data categories.

Total "Baseline" Requirement • **Usable Storage** • **# concurrent users**				
Primary Site				***Disaster Recovery Site***
Sandbox	**Development and Test**	**Pre-Production**	**Production**	**Production**
1 TB **3 con. users**	**6 TB** **10 con. users**	**100 TB** **25 con. users**	**100 TB** **50 con. users**	**100 TB** **50 con. Users**

Table 1: Baseline Requirement

3.2.2 Configuration and Capacity

3.2.2.1	The Contractor must provide a baseline Solution that is + or – 10% of the usable storage capacities as shown in Table 1 above.
3.2.2.2	The Contractor must identify the configuration and capacity of their Solution and all related components by product number, version number and description for the Primary site.
3.2.2.3	The Contractor must include a diagram that shows all related components required for the Primary site to interconnect within the environment as shown in Appendix 2 "Future Design Overview and Dataflow".
3.2.2.4	The Contractor must identify the configuration and capacity of their Solution and all related components by product number, version number and description for the Disaster Recovery site to be established at a separate location.
3.2.2.5	The Contractor must include a diagram that shows all related components for the Disaster Recovery site to interconnect within the environment as shown in Appendix 2 "Future Design Overview and Dataflow".
3.2.2.6	The Contractor must identify the configuration and capacity of their Solution and all related components by product number, version number and description for the Primary site to interconnect with the Disaster Recovery site.
3.2.2.7	The Contractor must include a diagram that shows all related components for the Primary site to link with the Disaster Recovery site within the environment as shown in Appendix 2 "Future Design Overview and Dataflow".

3.3 Scalability Requirement

If requested by Canada in a Task Authorization, the Contractor must provide a scaled Solution that is + or – 10% of the usable storage capacities for each of the separate environments as shown in Table 2 below. The scaled Solution shall include all hardware, software, licenses, integration services and connectivity between the Primary and Disaster Recovery sites.

Table 2 shows the scaling capacity requirements and the increased number of concurrent users for the scaled Solution.

Total "Scaled" Requirement • **Usable Storage** • **# concurrent users**				
Primary Site				***Disaster Recovery Site***
Sandbox	**Development and Test**	**Pre-Production**	**Production**	**Production**
5 TB 3 con. Users	20 TB 10 con. users	200 TB 25 con. users	200 TB 50 con. Users	200 TB 50 con. Users

Table 2: Scaled Requirement

3.3.1 Additional Scaling

If requested by Canada in a Task Authorization, Canada requires the Contractor to provide an increased scaling capability beyond the scaled capacities identified above to enhance both capacity and performance at the Primary and/or Disaster Recovery locations. The Solution shall include all hardware, software, licenses, integration services and connectivity to the Headquarters site as required.

3.3.1.1	The Contractor must identify whether their approach to scaling from 100 TB to 200TB and beyond would include removal and replacement of a previously supplied existing capacity with a higher capacity version or whether the increased scaled capacity would be an add-on to the existing capacity.

3.3.2 Configuration and Capacity

3.3.2.1	The Contractor must provide a scaled Solution that is + or – 10% of the usable storage capacities as shown in Table 2 above.
3.3.2.2	The Contractor must identify the configuration and capacity of their Solution and all additional related components by product number, version number and description for the Primary site to scale to the identified scaled level.
3.3.2.3	The Contractor must include a diagram that shows all additional related components and the associated connectivity required for the Primary site to scale to the identified scaled level within the environment as shown in Appendix 2 "Future Design Overview and Dataflow".
3.3.2.4	The Contractor must identify the configuration and capacity of their Solution and all additional related components by product number, version number and description for the Disaster

	Recovery site to the identified scaled level.
3.3.2.5	The Contractor must include a diagram that shows all additional related components and the associated connectivity required for the Disaster Recovery site to scale within the environment as shown in Appendix 2 “Future Design Overview and Dataflow”.
3.3.2.6	The Contractor must identify the configuration and capacity of their Solution and all additional related components by product number, version number and description for the Primary site to interconnect with the Disaster Recovery location at the identified scaled level.
3.3.2.7	The Contractor must include a diagram that shows all additional related components and the associated connectivity required for the above noted Primary site to interconnect with the Disaster Recovery site at the scaled level within the environment as shown in Appendix 2 “Future Design Overview and Dataflow”.
3.3.2.8	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.3.2.9	The Contractor’s Solution must automatically (without Canada’s internal resource intervention) rebalance/redistribute data across an expanded environment without the need to manually offload/reload data.
3.3.2.10	The Contractor’s Solution must not permit a degraded query response time from the query processing level regardless of the level of scale.
3.3.2.11	The Contractor’s Solution must enable scaling beyond 200TB to at least 600 TB of usable storage building upon the same underlying vendor technology as provided in the Contractor’s initial supplied configuration.
3.3.2.12	The Contractor must describe how they will scale from 200TB to at least 600TB as described in 3.3.2.11.

3.4 Query Processing

3.4.1	The Contractor must allow Canada to load applicable data into the Solution prior to handing off the Solution for testing on the identified queries scenarios.
3.4.2	**Query #1** The Contractor’s Solution must provide a combined elapsed time of 200 seconds or better to execute the 5 queries identified within the Definitions section of this SOR by utilizing the following process: • The 5 queries identified in the Query Pack will be submitted “back to back” serially and independently from five separate windows using the Contractor provided GUI based SQL interface. • When the first query finishes each subsequent query will be launched. • The elapsed time for each query to run and fetch the first 1000 rows of the result set will be captured. • The 5 individual query elapsed times will be summed and compared to the Contractor’s response to Article 3.4.3.
3.4.3	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.4.4	The Contractor must identify all related components which would be additionally required to further decrease query elapsed time as identified in the Contractor's response to Article 3.4.3
3.4.5	**Query #2** The Contractor's Solution must provide a combined elapsed time of 500 seconds or better to simultaneously execute the 5 queries identified within the Definitions section of this SOR by utilizing the following process: • The 5 queries identified in the Query Pack will be submitted serially from five separate windows by using the Contractor's provided GUI based SQL interface. • Queries to be executed roughly 1 second apart in a serial sequence from 1 to 5. • The elapsed time for each query to run and fetch the first 1000 rows of the result set will be captured. • The 5 individual query processing times will be summed and compared to the Contractor's response to Article 3.4.6
3.4.6	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.4.7	The Contractor must identify all related components which would be additionally required to further decrease the query elapsed time as identified in the Contractor's response to Article 3.4.6.
3.4.8	**Query #3** The Contractor's Solution must provide a combined elapsed time of 1,000 seconds or better to execute all of the 5 queries from the Query Pack simultaneously, wait 10 seconds then execute the same 5 queries simultaneously again by utilizing the following process: • For both runs, the 5 queries identified in the Query Pack will be submitted serially from five separate windows using the vendors provided GUI based SQL interface. • There will be a 10 second pause from end of 1st run to start of second run • For each of the two runs, the 5 queries are launched roughly 1 second apart in a serial sequence from 1 to 5. • The elapsed time for each query to run twice and fetch the first 1000 rows of the result set will be captured. • Total of all 10 queries will be summed and compared to the Contractor's response to Article 3.4.9
3.4.9	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.4.10	The Contractor must identify all related components which would be additionally required to further decrease the query elapsed time from the Contractor's response to Article 3.4.9.
3.4.11	**Query #4** The Contractor's Solution must not increase query response times by more than 10% when tables being queried begin receiving updates regardless of data size, by utilizing the following process: • One of the 5 queries in the query Pack will be submitted and a process will be started which will update approximately 1% of the records in one of the existing tables used in that query; • A comparison will be made to a baseline elapsed query time for same query without the update activities competition to determine any increased time factor; • The level of increase will be compared to the Contractor's response to one of the query processing times as selected by Canada.

3.5 Monitoring

3.5.1	The Contractor's Solution must include a monitoring component which is GUI based.

3.5.2	The monitoring component of the Contractors Solution must be configurable so that additional overhead may be minimized, (e.g. polling interval or number of metrics being collected).
3.5.3	The monitoring component must be able to monitor and report on: a. Hardware (E.G. CPU, disk, memory, network) utilization; b. Hardware errors; and **c.** Operating system errors.
3.5.4	T*echnical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.6 Usage Tracking (Real Time)

3.6.1	The Contractor's Solution must include real time performance measurement metrics for all of the following criteria: 1. The metrics must be visible using a graphical user interface (GUI). 2. The metrics must come from a central collection process that allows multiple users of the GUI to view the same metrics. 3. The polling interval for the metrics must be configurable. 4. The granularity (where applicable) of the metrics must be configurable using the GUI. 5. Real time metrics must include: a. CPU usage statistics; b. Memory usage statistics; c. Disk usage statistics; d. I/O statistics; and e. Active process metrics (e.g. queries, loads, backups): i. Statement being executed; ii. Number of rows being read from the database; iii. Number of rows being inserted; iv. Number of rows being updated; v. Number of rows being deleted; vi. Number of rows selected; vii. Elapsed time; viii. Associated USERID; and ix. Workload grouping (if applicable).
3.6.2	The Contractor must include a listing of all additional real time performance measurement metrics that can be accessed by Canada through the Contractor's Solution.
3.6.3	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.7 Usage Tracking (Historical)

3.7.1	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.7.2	The Contractor's Solution must include the capability for Canada to obtain resource usage reports over configurable time periods and granularities on memory, CPU, I/O, and storage

	utilization via a GUI interface.
3.7.3	The Contractor's Solution must include the capability for Canada to obtain workload based reports over configurable time periods and granularities via a GUI interface.
3.7.4	The Contractor's Solution must include the capability for Canada to produce data usage reports for data archival considerations.
3.7.5	The Contractor's Solution must include historical performance measurement metrics for all of the following criteria: 1. The metrics must be visible using a graphical user interface (GUI); 2. The GUI must include built-in reporting against the historical metrics; 3. The reporting time period must be configurable in the GUI, dynamically updating the report(s); 4. The reporting granularity must be configurable in the GUI, dynamically updating the report(s); 5. The metrics must come from a central repository that allows multiple users of the GUI to view the same metrics; 6. The retention period for the metrics must be configurable; 7. The granularity (where applicable) of the metrics in the repository must be; and 8. Historical metrics must include: a. CPU usage statistics; b. Memory usage statistics; c. Disk usage statistics; d. I/O statistics; and e. Process metrics (e.g. queries, loads, backups, etc.): i. Statement being executed; ii. Number of rows read from the database; iii. Number of rows inserted; iv. Number of rows updated; v. Number of rows deleted; vi. Number of rows selected; vii. Elapsed time; viii. Associated USERID; and ix. Workload grouping (if applicable).
3.7.6	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.7.7	The Contractor's Solution must include a facility that provides reports based on the historical statistics of executed queries.
3.7.8	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.7.9	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.7.10	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.7.11	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.7.12	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.7.13	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.7.14	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.8 Health/Event Monitoring

3.8.1	The Contractor's Solution must include a GUI capability which displays: 1. Information on warnings and abnormal events which may indicate a required intervention; 2. Information about critical and non-critical errors which will or may impact users; 3. Overall appliance health and allows user to drill-down to more detail on any monitored components; and 4. Information about appliance infrastructure incidents in detail.
3.8.2	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.8.3	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.9 Setup and Configuration Overhead

3.9.1	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.9.2	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.10 Central Management

3.10.1	The Contractor's Solution must include a GUI based management component which provides complete Solution management capabilities.
3.10.2	The management component of the Contractor's Solution must include role based access controls.
3.10.3	The management component of the Contractor's Solution must be available through GUI and command line interfaces.

3.10.4	The Contractor must identify any difference in capabilities in the command line verses the GUI.
3.10.5	The management component of the Contractor's Solution must include the ability to cancel any inflight database workload without jeopardizing the Solution's integrity.
3.10.6	The management component of the Contractor's Solution must include the ability to resume interrupted database workload without jeopardizing the proposed Solutions integrity.
3.10.7	The Contractor's Solution must allow Canada to terminate any process at any time without disrupting other non-related processes.
3.10.8	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.11 Data Technology and Integrity

3.11.1	The Contractor's Solution must generate a unique identifier thereby ensuring that each record in a table can be uniquely identified.
3.11.2	The Contractor's Solution must include the following capabilities: 1. Identify and resolve deadlock situations; 2. Enforce primary key constraints; 3. Enforce constraints to ensure that no duplicate values are entered in specific columns that do not participate in a primary key; 4. Enforce constraints on data values; 5. Enable and disable constraints; and 6. Assign user-defined default values to columns.
3.11.3	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.11.4	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.12 Database Access

3.12.1	The Contractor's Solution must include an Open Database Connectivity (ODBC) driver.
3.12.2	The Contractor's Solution must include a capability to execute dynamic SQL.
3.12.3	The Contractor's Solution must include a native call level interface that allows (or "includes") application programs access to function or procedures for processing dynamic SQL statements.
3.12.4	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.12.5	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.12.6	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.12.7	The Contractor's Solution must include a JDBC 2.0 or higher driver of type 2 or 4.

3.13 Tools

3.13.1	The Contractor's Solution must identify and include all relevant GUI based tools that enables tuning of the Solution.
3.13.2	The Contractor's Solution must include a GUI based capability that includes full lifecycle provisioning for DDL change management.
3.13.3	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.13.4	The Contractor's Solution must include a GUI based query capability.
3.13.5	The Contractor's Solution must include a GUI based capability which displays key metadata, metrics and statistics.
3.13.6	The Contractor's Solution must include a GUI based capability which gives the ability to prioritize specific workloads among all competing active workloads.

3.14 Utilities

3.14.1	The Contractor's Solution must enable utilities to be invoked from a GUI interface as well as direct command line mode.
3.14.2	The Contractor's Solution must include a data load utility which will spawn multiple concurrent processes to read from one input dataset to load a table without preventing queries on target table to be loaded.
3.14.3	The Contractor's Solution must include a data load utility that provides checkpoint re-start capabilities.
3.14.4	The Contractor's Solution must include any proprietary high speed adapters/interfaces necessary to achieve the fastest data loads possible with technology being proposed.
3.14.5	The Contractor's Solution must include integration with IBM's Infosphere Information Server Suite (Information Analyzer, Quality Stage and Data Stage). The tools mentioned above must be able to access metadata from the Contractor's Solution and must be able to bulk load data into the Contractor's Solution.
3.14.6	The Contractor's Solution must be integrated with IBM's Infosphere Information Server (IIS) within 6 months of General Availability of a new IIS release.
3.14.7	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*

3.15 Backup and Recovery

3.15.1	The Contractor's Solution must include capability to allow backups taken at table or database level of granularity to be used for restore of same object in another database of same

	technology.
3.15.2	The Contractor's Solution must integrate with the current backup Solution which is currently Tivoli Storage Management.
3.15.3	The Contractor's Solution must backup and restore at a minimum rate of 4 TB an hour.
3.15.4	The Contractor's Solution must meet a "Recovery Point Objective" (RPO) of the last successfully loaded/inserted/updated or deleted data in case of any Solution failure where it is not immediately re-startable and recovery is necessary.
3.15.5	The Contractor's Solution must include the capability to backup: 1. an entire database; 2. a single table; 3. a set of tables; and 4. part(s) of a table.
3.15.6	The Contractor's Solution must include the capability to incrementally backup: 1. an entire database; 2. a single table; 3. a set of tables; and 4. part(s) of a table where only the changes to the database or tables are backed up.
3.15.7	The Contractor's Solution must include the capability to allow read and write access to tables during a backup of the same tables.
3.15.8	The Contractor's Solution must include the capability to display metadata about the backups that have been taken. Metadata must include: 1. When the backup was started; 2. When the backup completed; 3. The type of backup; 4. The database and tables included in the backup; and 5. The size of the backup.
3.15.9	The Contractor's Solution must include the capability to restore and recover: 1. a complete database; 2. a single table; 3. a set of tables; and 4. part of a table.
3.15.10	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.15.11	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.15.12	The Contractor's Solution must include a capability which ensures that in any crash recovery scenario that data integrity is maintained and the database remains in the same state as it was just prior to the point before the crash occurred.
3.15.13	*Technical requirement to be inserted based on results of POP testing from the successful*

	Bidder. Please see Point-Rated Technical Requirements for details.
3.15.14	The Solution must meet a "Recovery Time Objective" (RTO) from time of failure and be returned to a fully operational state within the following timelines: a. Severity Level 1 (if supporting critical queries): 4 hours b. Otherwise: 24 hours

3.16 Primary Site Availability

3.16.1	The Contractor's Solution must offer redundancy of all physical components such that there is no single point of failure.
3.16.2	The Contractor's Solution must maintain availability of 99.95% over a 24/7, 365 day cycle (outside scheduled shutdowns) of components at the Primary Site location..
3.16.3	With respect to the primary site availability, the Solution must meet a "Recovery Time Objective" (RTO) from time of failure and be returned to a fully operational state within the following timelines: a. Severity Level 1 (if supporting critical queries) 4 hours b. Otherwise: 24 hours
3.16.4	The Contractor's Solution must identify and include all necessary components to implement a hot-site failover in a secondary data center in the case of the critical data marts not being recoverable within 4 hour RTO.
3.16.5	The Contractor's Solution must meet a "Recovery Point Objective" (RPO) of the last successfully loaded/inserted/updated or deleted data in case of any Solution failure where it is not immediately re-startable and recovery is necessary.

3.17 Disaster or Elongated Outage Availability

3.17.1	The Contractor's Solution must offer a redundant system at the Disaster Recovery Site such that there is no single point of failure.
3.17.2	The Contractor's Solution must include an automatic data replication/migration process to be initiated from the Primary database to the Disaster Recovery database.
3.17.3	The Contractor's Solution must include a pre-packaged or database provided mechanism to keep the critical data mart(s) at the Disaster Recovery site up to date automatically without Canada's internal resource development.
3.17.4	The Contractor's Solution must ensure that the process identified in Articles 3.17.2 and 3.17.3 takes no more than 5 minute data latency from Primary database to the Disaster Recovery database.
3.17.5	The Contractor's Solution must maintain availability of 99.95% over a 24/7, 365 day cycle (outside scheduled shutdowns) of components at the Disaster Recovery location.
3.17.6	In case of a required recovery scenario affecting only the Disaster Recovery site - all Solution components at that site must meet a "Recovery Time Objective" (RTO) of 4 hours from time of failure inclusive of the Disaster recovery database being re-synced with primary DB.
3.17.7	The Contractor must include a diagram representing the physical design of their Solution and

	provide a list of hardware and software components that would facilitate the hot-site failover capability.
3.17.8	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.17.9	The Contractor's Solution must meet a "Recovery Point Objective" (RPO) of the last successfully loaded/inserted/updated or deleted data in case of any Solution failure where it is not immediately re-startable and recovery is necessary.

3.18 Data Dictionary

3.18.1	The Contractor's Solution must include a catalogue (or data dictionary) capability that is updated automatically each time Data Definition Language (DDL) is applied.
3.18.2	The Contractor's Solution must include SQL query able metadata that is updated automatically in real-time each time Data Definition Language (DDL) and Data Manipulation Language (DML) is executed on the database.
3.18.3	The Contractor's Solutions must include the capability to access the catalogue and retrieve information related to database objects.

3.19 General Security Requirements

3.19.1	The Contractor's Solutions must include an audit capability which records the following information for the database updates, insertions, deletions and selects by individual users on individual objects: a. Database USERID (ID as stored in the database); b. Date/time stamp (date and time of action); c. Transaction type (select, insert, update, or delete); d. Database Name; e. Target object(s); and f. DML submitted.
3.19.2	The Contractor's Solution must provide external access to security audit information through one or more of the following methods: syslog logging to a remote system, ODBC database access, SNMP Trap messages, Microsoft Windows Event log, or Text based log file that is software readable.
3.19.3	The Contractor's Solution must record security events in system log files.
3.19.4	The Contractor's Solution must have audit records including the following event data: event(s) occurred, source(s), outcome, identity, and type.
3.19.5	The Contractor's Solution must provide time stamps for audit records.
3.19.6	The Contractor's Solution must provide user activity auditing that provides an administrator the ability to determine all commands which have been run by a user.

3.19.7	The Contractor's Solution must have logs that are in human readable form and if binary format logs are used, there must be an application included that translates these into human readable format in near real-time (i.e. as soon as created the binary format is translated within a few seconds to human readable format)
3.19.8	The Contractor's Solution must record the SIEM event severity level in the security log
3.19.9	The Contractor's Solution must ensure that violations of access control events are recorded.
3.19.10	The Contractor's Solution must ensure that security event logs containing any number of events are not overwritten before archival. Minimum archive period is 36 hours.
3.19.11	The Contractor's Solution must ensure SIEM log file integrity.
3.19.12	The Contractor's Solution must record relevant data or detail concerning security events such as: IP addresses, user identity, port, file name, path, and trusted time stamp.

3.20 Access Control

3.20.1	The Contractor's Solution must integrate with LDAPv3-Compliant Directory.
3.20.2	The Contractor's application software must require a user name and password login.
3.20.3	The Contractor's Solution must prompt the user to enter and confirm a new password on the date the old password expires if credentials are stored locally.
3.20.4	The Contractor's Solution must enable passwords to expire at various times as predetermined by Canada if credentials are stored locally.
3.20.5	The Contractor's Solution must permit only one instance of a password per account at any given time.
3.20.6	The Contractor's Solution must not allow any operation to be performed on any database object unless the user is authorized to conduct the operation concerned.
3.20.7	The Contractor's Solution must include the ability to enable adjustment to the degree of details captured by the auditing capability as required.
3.20.8	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.20.9	The Contractor's Solution must allow the functionality to set the length of time that the user's password(s) will be valid.
3.20.10	The Contractor's Solution must include the user with the option to set the number of failed access attempts that will be allowed.
3.20.11	The Contractor Solution must support authentication at the application level using user-ID and password and at the network level using a VPN Client and token.
3.20.12	The Contractor's Solution must include integration with CA E-trust Directory LDAP for authorization and authentication to the Solution.

3.20.13	*Technical requirement to be inserted based on results of POP testing from the successful Bidder. Please see Point-Rated Technical Requirements for details.*
3.20.14	The Contractor must read, sign and adhere to an Acceptable Use Policy (AUP) when accessing DCH, DCSL and/or DCWQ data centres**.** See Appendix 5.

3.21 Operating Software and Software Upgrades

3.21.1	The Contractor must provide Canada with End User License Agreements for all commercial and shareware software products acquired for use with the Solution. See Appendix 3 for definition of Software.
3.21.2	The Contractor must complete the installation and regression testing of any software upgrades during the, warranty period or any period of Maintenance and Support service during the life of the contract and all extensions issued thereto.
3.21.3	The Contractor's Solution must work with and must not interfere with Canada's software.
3.21.4	The Contractor must provide Canada with the right to subject any software upgrades to an acceptance process and approval.
3.21.5	The Contractor must, prior to installation of any software upgrade, provide Canada with a copy of their software release notes that identify the new software version numbers, any changes incorporated into the software upgrade, any issues or deficiencies the upgrade has corrected, and any outstanding issues or problems that are still open.
3.21.6	The Contractor must provide Canada with the opportunity to perform any testing deemed necessary to proposed software upgrades before deployment.
3.21.7	The Contractor must support regular updates to the software used by the Solution.
3.21.8	The Contractor must address any known vulnerabilities within their software and agree to address any 3rd Party software vulnerabilities used within the Solution within 30 days from date of identification.
3.21.9	The Contractor must identify and include all application software upgrades based on the Contractor's recommendation and Canada's acceptance of that recommendation through the warranty period or during the period of any extended Maintenance and Support.
3.21.10	The Contractor must provide a minimum of 3 years support on previous versions of their software.
3.21.11	The Contractor must guarantee the safety and integrity of the data stored on the Solution during any upgrade activities.
3.21.12	The Contractor must describe in sufficient scripted detail and documented illustration, their application upgrade procedures, data integrity precautions and the recovery procedures in the event of an upgrade failure.
3.21.13	The Contractor must acknowledge that Canada's current platforms can be changed at any time and that the Contractor must work with the Technical Authority to resolve any software integration issues over the life of the Contract and any extensions issued thereto.

3.21.14	Shipment and delivery services by the Contractor for software updates must include: • Packaging all software and licenses; • Associated Commercial Documentation; • Prepare and submit any necessary Canadian and US Customs forms; • Identify and contract for any required broker services; • Insure all shipped goods, for full value, either with the shipper or self-insure them as per your corporate policy; • Ship the material with a bill of lading that corresponds to the shipping package tracking number; delivery site; commercial software product, version, and serial number; proprietary software version and any serial numbers; and BOM item number for use by Canada in verifying the receipt of all shipped software; and • Fax a copy of the Bill of Lading to Canada at the time of the shipment(s).
3.21.15	The Contractor must provide all appropriate end user license agreements at no cost to Canada.
3.21.16	The Contractor must provide Canada with End User License Agreements for all commercial and shareware software products acquired for use with the procured Solution.
3.21.17	The Contractor must provide, as part of the Contract and any extensions issued thereto, all appropriate upgrades at no cost to Canada resulting from the following: • patches and newer versions of software to eliminate failures or bugs discovered by the vendor; • provision of software to support new hardware, substituted by the vendor; and • maintain support and interoperability between newer and older versions of hardware and software.

3.22 Network Environment

3.22.1	The Contractor's Solution must include the capability for backups to be sent directly to Canada's current backup Solution "IBM's Tivoli Storage Manager" by using the SAN fabric connection (not over network).
3.22.2	The Contractor's Solution must connect to the network using either 1Gb copper or 10Gb SFP fiber optics connections.
3.22.3	The Contractor's Solution must have redundant network ports in order to remain operational in the event of a Network Interface Card (NIC) failure.
3.22.4	The Contractor's Solution must have a separate network connection for hardware management that is completely isolated from the NIC's used to transmit data. The concept of hardware management network or lights out management. Allowing remote power on/off, reboots, firmware upgrades and other similar functions.
3.22.5	The Contractor must ensure that the power and cooling units of primary site Solution is bottom-vented, and the disaster recovery site is top-vented.
3.22.6	The Contractor's Solution must have all devices come with dual power and dual NIC connections.
3.22.7	*The Contractor's Solution* must have electrical connections tiered, so that if one connection fails on one grid, the other active connection will still support the entire unit at full power.
3.22.8	The Contractor's Solution must have power supplies supporting both single and three-phase power.

3.22.9	The Contractor's Solution must have all devices in the DC (Data Centre) operating at a minimum of 230 volts.
3.22.10	The Contractor's Solution must have power connectors from the customer equipment to our internal grid and supporting L6 type connectors.
3.22.11	The Contractor must ensure that all devices and power units are CSA (Canadian Safety Associated) approved.
3.22.12	The Contractor must ensure that any devices which are not self-standing comply with standard 19" rack mount systems.
3.22.13	The Contractor must ensure that all devices other than self-standing must be rack mountable and not exceed 42" in depth
3.22.14	The Contractor must ensure that all Solution components fit through the Data Centres access doorway systems which are 53" x 81" in sizing.
3.22.15	The Contractor must ensure that the Solution complies with a cooling system with a hot and cold aisle system using air.

3.23 Technical Documentation

3.23.1	The Contractor must identify all documentation that is available and would be included to Canada in support of each element of the Solution.
3.23.2	The Contractor must include all documentation written in English.
3.23.3	The Contractor must allow Canada to internally host the documentation internally for multi-user access to support the Solution.
3.23.4	The Contractor must provide Canada with accessibility to all documentation updates covering enhancements and/or replacement releases within 10 days following release of General Availability announcement.
3.23.5	The Contractor must identify the format in which all documentation updates covering enhancements and/or replacement releases will be made available.

4.0 Corporate Requirements

4.1 General Requirements

4.1.1	The Contractor must include project management services to plan, monitor, report, track, and manage the successful delivery, integration and testing of the Solution. As part of the project management plan, the Contractor must describe the approach to be taken by the project management resource to implement, manage, resolve, and report on issues/problems and risk management procedures.
4.1.2	The Contractor must address potential risks to the project and how they will identify and assess risks, mitigation strategies, eliminate or minimize, and recover from identified risks.

4.1.3	The Contractor must define how they will ensure that project documents and data are controlled for the life of the contract including all extensions issued thereto.
4.1.4	The Contractor must identify an escalation process that exists within their corporate structure to which issues can be elevated up to and including senior corporate management in the event considered necessary.

4.2 Contractor Resources

4.2.1	The Contractor must identify and provide Canada with one or more project resource(s) that will be responsible for overseeing the delivery, integration and acceptance testing of the Solution. This resource(s) will be responsible for performing the following project managerial and technical responsibilities, but not limited to: a. Work with Canada to align the Contractor activities and deliverables with the Contractor's project plan, schedule and requirements; b. Work with Canada to implement processes that will ensure that the Contractor can interface with Canada to address delays, issues, and address any issue needing correction; and c. Provide technical services on an as and when requested basis to assist with the development of the interface and the overall integration and exploitation of the Solution.
4.2.2	The primary and back up Project Manager and Systems Engineer/Integration Specialist must have an approved Canadian Government security clearance at the Enhanced Reliability level.
4.2.3	The Contractor's primary and back up Project Manager must have the following minimum qualification: • a minimum of 5 years of experience within the last 8 years in integrated appliance technology on a similar delivered project with similar related duties.
4.2.4	The primary and backup Systems Engineer/Integration Specialist must have the following minimum qualification: • a minimum of 3 years of experience within the last 3 years in the installation, configuration, troubleshooting, performance analysis and tuning of in integrated appliance technology on a similar delivered project.
4.2.5	For the duration of the Contract and any extensions issued thereto, the Contractor must include: a. Support for all technical and non-technical inquiries; b. A representative who will coordinate information between the Technical Authority and the Contractor with respect to Contract Deliverables, Technical Substitutions, Problem Reports, and Certification.
4.2.6	The Contractor must identify the corporate resource that will coordinate information to the Technical Authority with respect to Contract Deliverables, Technical Substitutions, Problem Reports, and Certification.
4.2.7	The Contractor, at their own expense, must attend progress review meetings with the Technical Authority. Meetings will be held at a location as specified by the Technical Authority.

5.0 Warranty

The Contractor must provide a 12-month warranty as follows:

5.1	The Contractor's 12 month warranty services period must be included for all Solution delivered software, firmware and hardware as established following completion of the POP testing process.
5.2	The Contractor's 12 month warranty coverage must include any application software and/or firmware upgrades required to support revisions to the Solution.
5.3	The Contractor's 12 month warranty coverage must include all on-site remedial software, firmware and hardware support as well as telephone or online support.
5.4	The Contractor's Solution must maintain an availability level of 99.95% percent during the Contractor's warranty period.
5.5	In regards to the warranty, the Solution must meet "Recovery Time Objectives" (RTO) from time of failure and be back operational from time of notification by Canada during the life of the Contract or any extensions issued thereto in accordance with the following timelines: a. Level 1 (if supporting critical queries): 4 hours b. Otherwise: 24 hours
5.6	The Contractor's warranty requirements must include: a. Call Center support to include: ▪ toll free phone support; ▪ telephone based technical support for critical outages 24/7, 365 days a year; ▪ On site reSolution as required; ▪ If the Customer Support Center is not able to resolve the issue within 1 hour then the next level of support will be applied; and ▪ Regular repair or replacement of failed parts and software maintenance/upgrades. Canada reserves the right to elevate an issue to higher support levels.
5.7	The Contractor's warranty coverage must include on-site preventive maintenance and remedial hardware, firmware and software support as well as telephone or online support for all delivered hardware and software at no additional cost to Canada.
5.8	The Contractor must furnish all labour and Solution components required to restore the Solution to a fully operational condition during the warranty period.
5.9	The Contractor must identify the 1-800 call intake centre phone number to which the GOC will make the initial call for warranty service.
5.10	The Contractor must include Technical Support Services during the warranty period at no additional cost to Canada.
5.11	The Contractor must include warranty services to investigate specifics about the functioning of covered products to determine whether there is a defect in the Solution.
5.12	The Contractor's responsibilities to include Technical Support Services must be limited to the current Standard Release plus the two (2) prior Standard Releases (collectively referred to as "Covered Standard Releases").

5.13	The Contractor's Solution must meet a "Recovery Point Objective" (RPO) of the last successfully loaded/inserted/updated or deleted data in case of any Solution failure where it is not immediately re-startable and recovery is necessary.

6.0 User Training

The Contractor must provide Canada with user training as requested in a Task Authorization issued by Canada on an as-and-when requested basis as follows:

6.1	The Contractor must include training for all components of the Solution.
6.2	The Contractor must identify all of their training programs available for systems users and technical support relative to the identified requirement.
6.3	The Contractor must include a comprehensive draft training strategy plan for Canada's review and approval.
6.4	The Contractor must provide user training in English as requested by Canada.
6.5	The Contractor must identify the methodology (ies) which are available to Canada for their training programs (I.E. Hard copy, CD-ROM, online, etc.).
6.6	The Contractor must include training documentation in English to train resources on the technical use, configuration, troubleshooting and maintenance of the Contractor's Solution, within 10 calendar days following contract award.
6.7	The Contractor must modify the Training Plans as required by Canada.
6.8	The Contractor must include the right for Canada to copy the training material for Canada's internal mentoring and training.

7.0 Maintenance and Support

The Contractor must provide Canada with maintenance and support services as requested in a Task Authorization issued by Canada on an as-and-when requested basis as follows:

7.1	The Contractor must identify all of the various Solution support programs and associated terms and conditions that they have available to provide Maintenance and Support services following the Warranty period.
7.2	The Contractor's Solution must maintain an availability level of 99.95% during the life of the contract and any extensions issued thereto.
7.3	Maintenance and support coverage must begin immediately at the end of the Contractor's 12 month warranty period should Canada exercise the option.
7.4	In regards to the maintenance and support, the Solution must meet "Recovery Time Objectives" (RTO) from time of failure and be back operational from time of notification by Canada during the life of the Contract or any extensions issued thereto in accordance with the following timelines:

	a Level 1 (if supporting critical queries): 4 hours b Otherwise: 24 hours
7.5	The Bidder's Solution must meet a "Recovery Point Objective" (RPO) of the last successfully loaded/inserted/updated or deleted data in case of any Solution failure where it is not immediately re-startable and recovery is necessary.
7.6	The Contractor must include continuous effort to repair a reported problem during the Principal Period of Maintenance (24 hours a day, 7 days a week for 365 days a year)
7.7	The Contractor must ensure the Solution can be returned to fully functional capability within the timeframes identified in Article 7.4 from time of notification by Canada during the life of the Contract or any extensions issued thereto.
7.8	The Contractor's maintenance and support requirements must include the following during the life of the Contract or any extensions issued thereto: Call Center support to include: ▪ 1-800 phone support; ▪ telephone based technical support for critical outages 24/7, 365 days a year; ▪ On site reSolution as required; ▪ If the Customer Support Center is not able to resolve the issue within 1 hour then the next level of support will be applied; and ▪ Regular repair or replacement of failed parts and software maintenance/upgrades. Canada reserves the right to elevate an issue to higher support levels.
7.9	The Contractor's maintenance coverage must include on-site preventive maintenance and remedial software, firmware, hardware and overall Solution support during the life of the contract and any extensions issued thereto.
7.10	The Contractor must furnish all labour and parts required due to normal wear to restore the Solution to a full operating condition during the life of the Contract and any extensions issued thereto, at no additional cost to Canada.
7.11	All of Canada's requests for services must be made initially to the call intake centre whose number the Contractor will provide to Canada prior to commencement of services.
7.12	The Contractor must include Technical Support Services and correction of Residual Errors during the Principal Period of Maintenance (PPM).
7.13	The Contractor must include Technical Support Services during the life of the Contract and any extensions issued thereto to investigate specifics about the functioning of the Solution to determine whether there is a defect in the Solution.
7.14	The Contractor must include available Product Releases, in accordance with Supplemental General Conditions, 4004 (2010-08-16) – Maintenance and Support Services for Licensed Software. Any such services will be performed in accordance with a mutually-agreed schedule.
7.15	The Contractor must provide a minimum of 3 years support on previous versions of their software.
7.16	The Contractor's Solution or any component of the Solution must be supported for a minimum of 3 years from date of installation.

7.17	The Contractor's Technical Support Services must be limited to the current Standard Release plus the two (2) prior Standard Releases (collectively referred to as "Covered Standard Releases") during the life of the Contract and any extensions issued thereto.
7.18	Notwithstanding Article 7.16, the Contractor must include Technical Support Services during the life of the Contract and any extensions issued thereto for a Standard Release that precedes the Covered Standard Releases unless such error has been corrected by a Covered Standard Release.
7.19	At Canada's request, the Contractor must include during the life of the Contract and any extensions issued thereto: (a) a current list of compatible hardware operating system releases, if applicable; and (b) a list of the Contractor's Software Supplemental or Standard Releases.
7.20	The Contractor must work with Canada's technical resources for the duration of the Contract and any extensions issued thereto to include Canada's technical resources with hands on technical familiarization and knowledge transfer for the delivered Solution.
7.21	The Contractor must agree to an annual review of the maintenance and support included for the previous contract year by Canada during the life of the Contract and any extensions issued thereto.

8.0 Security

The Contractor must provide Canada with a plan that documents the procedure to verify each verifiable security control in both Appendix 7 – Media Protection Security Control Policy and Appendix 8 - Security Controls Profile.

The Contractor must implement the plan and provide Canada with a report that includes the procedure to confirm that the security safeguard, associated to a security control in both the Appendix 7 – Media Protection Security Control Policy and Appendix 8 - Security Controls Profile is implemented correctly and satisfies applicable standards as specified in the service design specifications.

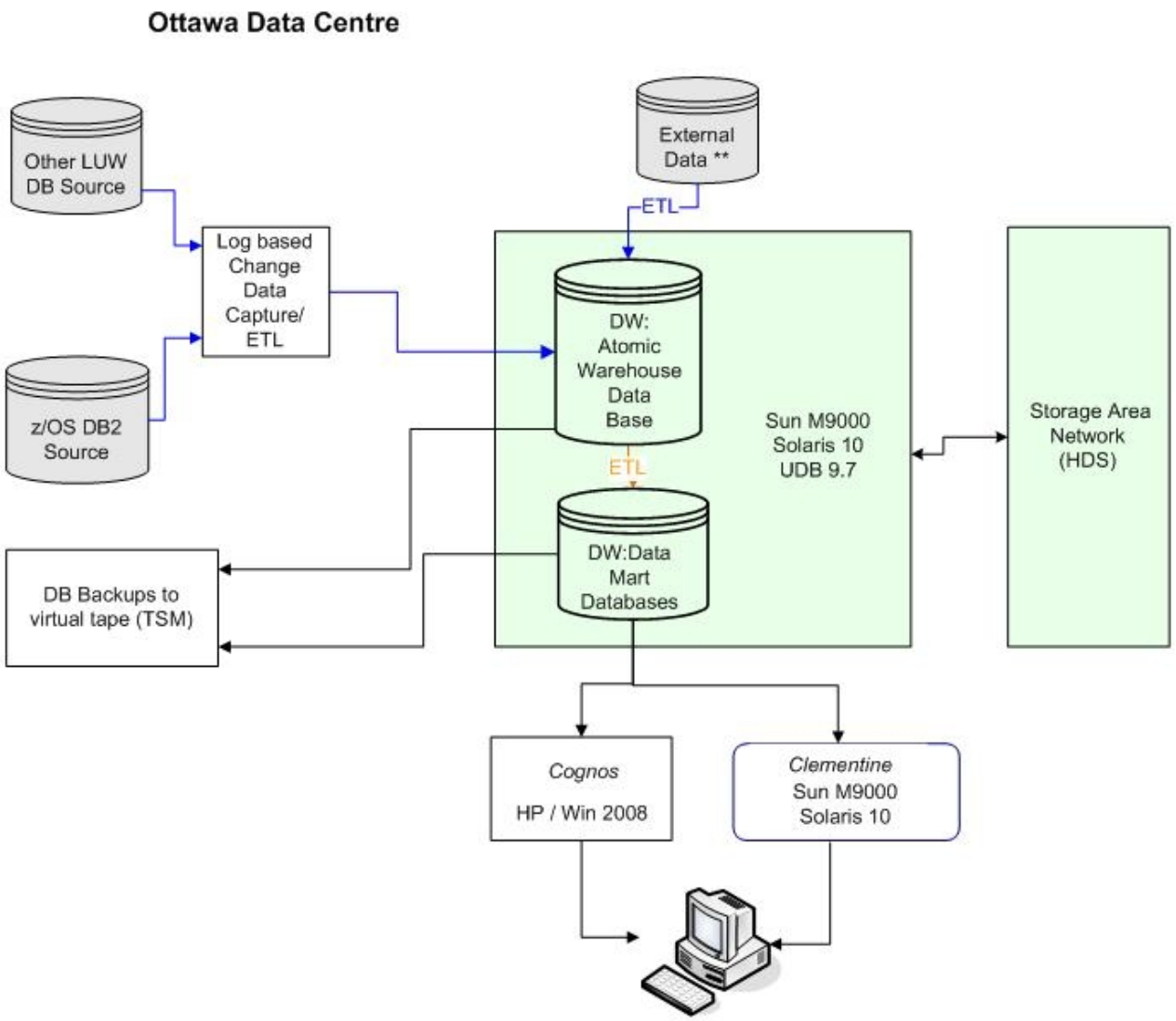
Appendix 1 Current Canada Environment (*Page 1 of 2)*

Current Mainframe Platform
Database Environment (Tier 3)
Hardware: **Operating System: ZOS** **IBM DB2 database V10**
Current DW Foundation Platforms
Database Environment (Tier 3)
Hardware: Sun M9000 frame **Operating System: Sun Solaris V10** **IBM DB2 database V9.7**
Current Workstation Platform (Tier 1)
Standard X86 Windows 7
Analysis and Reporting Platform (Tier 2)
Hardware: Intel Xeon or Itanium **Operating System: Windows 2008 Server Standard Edition SP 2 64 Bit. Special build with the addition of IIS as well as Configuration Script for Cognos.** **Hardware : Sun M9000** **Operating System: Sun Solaris V10**
Software Tools
Data Management Tools – IBM DataStage, QualityStage, Information Analyzer **IBM Change Data Capture for z/OS** **IBM FastTrack Metadata – Metadata WorkBench, Business GlossaryData Mining – Clementine** **Business Research - Impromptu** **Business Analytics – Impromptu** **Text Analytics – OmniFind LanguageWare** **Identity Resolution – Identity Insight** **Reporting – Cognos 8, Report Studio** **BI Portal - Cognos Connection** **OLAP - Powerplay Studio, Analysis Studio** **Cube - Cognos Transformer** **Performance Metrics/Scorecarding - Metric Studio** **Event Capture/Processing - Event Studio** **View Management -Virtual View Manager** **Business Objects**
Data Sources
Sybase ASE **DB2 on z/OS, Solaris, Windows** **CA-IDMS** **Microsoft SQL** **Oracle** **flat files** **VSAM** **PostgreSQL**

Crown resources currently update the Data Warehouse with fresh data on a periodic basis (i.e. daily, weekly) during batch windows.

Current Canada Environment (*Page 2 of 2*)

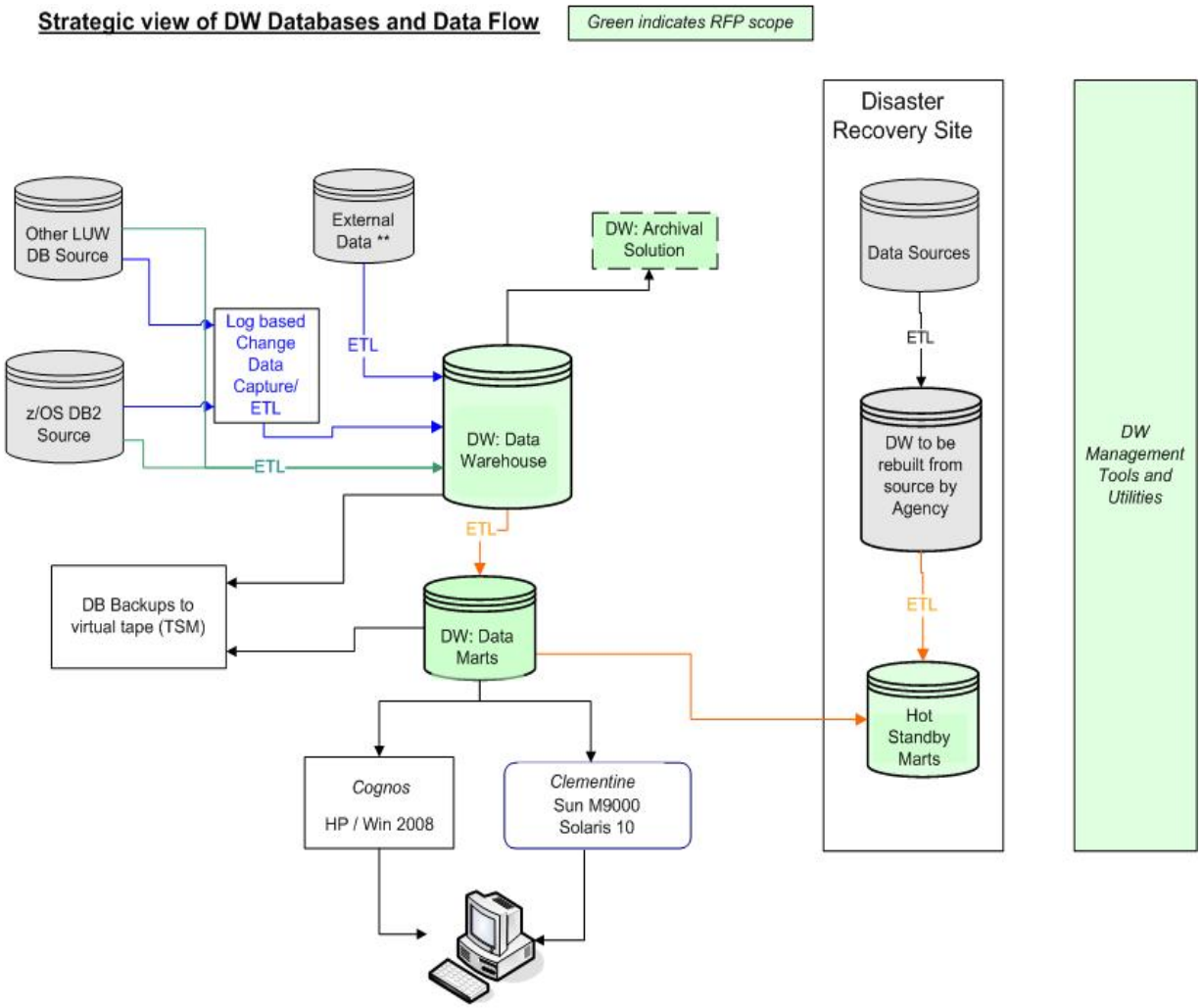
Current view of DW Databases and Data Flow



*** External data as referenced in this diagram references data originating external to CBSA but subsequently stored inside the Agencies firewall.*

Appendix 2 Future Design Overview and Dataflow

The following diagram includes a strategic view of Canada's future Data Warehouse. This environment could change during the life of the contract.



** External data as referenced in this diagram references data originating external to CBSA but subsequently stored inside the Agencies firewall.

Appendix 3 Definitions

Appliance	An appliance is a preconfigured bundle of hardware and software integrated at the factory, and typically packaged with services at time of sale.
Appliance Based	A preconfigured bundle of hardware and software integrated at the factory, created for a specific purpose but built and optimized at the Client Site.
Availability	The assurance that an IT infrastructure has suitable recoverability and protection from system failures, natural disasters or malicious attacks
99.95% Availability	Regardless of the availability percentage of 99.95%, the solution must meet the "Recovery Time Objectives" (RTO) from time of failure and be back operational in accordance with the following timelines: Level 1 (if supporting critical queries) 4 hours ; Otherwise: 24 hours
COTS system	A non-developmental item of supply that is generally available and sold in the commercial marketplace, and that can be procured or utilized under government contract in the same precise form as available to the general public.
Checkpoint re-start	Recovering from a system failure.
Client Site	SSC locations in the National Capital Region
Client Disaster Recovery location	A federal government facility within the National Capital Area
Client Primary location	A federal government facility within the National Capital Area
Client User	Employees of the Government of Canada and other individuals authorized by the client to perform services in relation to the business and affairs of the client, including Contractors or consultants performing work for the client from time to time.
Critical Data Mart	A Data Mart with a higher expectancy of availability at the primary Client Site; the contents of which are to be automatically associated with the Disaster Recovery/Elongated Outage environment.
Data Mart	The data mart is a subset of the data warehouse that is usually oriented to a specific business line or team.
Data Warehouse	A centralized repository which contains a collection of data, pulled from multiple sources, used to satisfy the business intelligence needs of the user.

Data Warehouse Environment	The complete domain and consists of the 3rd tier, 2nd tier and 1st tier hardware/software used to include an integrated business intelligence solution.
Data Warehouse Foundation	A sub-set of the Data Warehouse Environment and consists primarily of the 3rd tier which is the data warehouse. Data Marts and required hardware and software deemed necessary to support those components.
Development and Test	The Development and Test environment is a specific part of the solution used by administrators and developers to test new releases without impacting end users.
Disaster Recovery	The Disaster Recovery environment is a specific part of the solution used by administrators and end users when an incident at the primary site makes the primary site inaccessible or dysfunctional.
1st Tier	Presentation Tier – tier that interacts with the end-user.
2nd Tier	Application Tier – middle tier – consists of the application server platform(s) and will support COTS based apps used to access and manage the third tier.
3rd Tier	Data tier – bottom tier – consists of the database(s) of the Data Warehouse and Data Marts.
Elongated Outage	A variable time period as determined by Canada which results in an unacceptable loss of availability to client.
Extract-Transform-Load	Extracts data from multiple sources, transforms it to fit business needs, and ultimately loads it into the data warehouse. IBM's Infosphere Information Server (Data Stage) or higher will continue to be used for this function. .
GUI capability	A graphics-based operating system interface that uses icons, menus and a mouse (to click on the icon or pull down the menus) to manage interaction with the system
Insert/Update workload	Insert/update workload will consist of one insert/update process/job.
Integration Services	System integration and testing will be the first step in the POP and Acceptance Test procedures following delivery of the Contractor's solution at destination.
Lifecycle Provisioning	Function of introducing a changed or new component into a lower environmental state and migrate it to higher state(s) by a controlled, tested and repeatable process.
Management Tools	Tools to enable centralized management of the installed infrastructure.
National Capital Region (NCR)	An official federal designation for the Canadian capital of Ottawa, Ontario, the neighbouring city of Gatineau, Quebec, and surrounding urban and rural communities within 60 km of Ottawa.
Network Addressable	A device viewable from any point on the network
Operational Environments	The required solution will be in support of 5 separate environments consisting of Sandbox, Development/Testing, Pre-production, Production and remote Disaster Recovery.

Performance Measurement Metrics	Data captured to aid the process of performance analysis.
Pre-Production	The Pre-Production environment is a specific part of the solution used by administrators and testers to test new releases without impacting end users.
Principal Period of Maintenance & Support	The identified timeframe under which the solution must be supported by the Contractor.
Production	The Production environment is a specific part of the solution used by administrators and end users which will house production data.
Query 1	Query 1 is a 2 way table-join where the number of rows on tables approximate 510,000,000 and 176,000,000 and size is 84GB and 30GB respectively.
Query 2	Query 2 is a 3 way table-join where the number of rows on tables approximate 62,000,000, 278,000,000 and 176,000,000 and size is 38GB, 34GB and 30GB respectively.
Query 3	Query 3 is a 11 way table-join where the number of rows on tables approximate 176,000,000, 278,7000,000, 171,00,000, 900,000,000, 944,000,000, 1,900,000, 487,000,000, 200,000,000, 18,000,000, 60,000,000 and 511,000,000 and size is 30GB, 34GB, 44GB, 142GB, 180GB, 1GB, 61GB, 28GB, 3GB, 13GB, and 84GB respectively.
Query 4	Query 4 is a 3 way table-join where the number of rows on tables approximate 62,000,000, 278,000,000 and 176,000,000 and size is 38GB, 34GB and 30GB respectively (***predicates differ from Query #2***).
Query 5	Query 5 is a 10 way table-join where the number of rows on tables approximate 176,000,000, 278,000,000, 172,000,000, 885,000,000, 944,000,000, 1,866,000, 487,000,000, 200,000,000, 18,000,000, and 60,000,000 and size is 30GB, 34GB, 44GB, 142GB, 180GB, 1GB, 61GB, 28GB, 3GB, and 13GB respectively
Ready for Use (RFU)	The product is delivered, installed, powered up, visible on the SSC network and configured for Canada client use as per the vendor's specifications.
Real Time vs Historical Time	Real time refers to events in flight or execution status whereas "historical" refers to events or processes that have already finished.
Recovery Point Objective (RPO)	The maximum tolerable period in which data might be lost due to an incident.
Recovery Time Objective (RTO)	The duration of time and a service level within which a business process must be restored after a disruption in order to avoid unacceptable consequences associated with a break in business continuity.
Repeated Execution Query	A query resubmitted where only the values of the predicate arguments have been changed.
Rogue Processes	Those processes which consume an abnormally large amount of resources and may

	threaten the systems availability.
Sandbox	The sandbox environment is a specific part of the solution used by administrators to test new releases without impacting developers or end users.
Scheduled Downtime	Scheduled Downtime is a result of maintenance that is disruptive to system operation and usually cannot be avoided with a currently installed system design. Scheduled Downtime events might include patches to system software that require a reboot or system configuration changes that only take effect upon a reboot. In general, Scheduled Downtime is usually the result of some logical, management-initiated event.
Seamless Integration	The ability to interoperate with an existing component in such a way that the existing component(s) need not be modified to achieve full optimal functionality of either component.
Security Information and Event Management	An approach to security management that seeks to provide a holistic view of an organization's information technology.
Service Levels	The performance goals of business processes to meet established objectives.
Software	Is defined for this purpose as commercial off-the-shelf software, proprietary software, shareware, freeware, open source and data sets. Software is defined for this purpose as commercial off-the-shelf software, proprietary software, freeware, and data sets
Solution	The cumulative and integrated combination of hardware and software supplied by the Contractor meeting all requirements in the SOR.
Sufficient Scripted Detail	Include a capability for the evaluation team to fully understand the manner in which the solution meets the requirement through the use of wording and/or illustrations.
Unscheduled Downtime	The solution is not available when it is supposed to be.

Appendix 4 Abbreviations

BI	Business Intelligence
CBSA	Canada Border Services Agency
DBA	Database Analyst *(Internal to the Agency)*
DBMS	Database Management System
DDL	Data Definition Language
DRDA	Distributed Relational Database Architecture
DWBI	Data Warehouse Business Intelligence
DW	Data Warehouse
DWF	Data Warehouse Foundation
GUI	Graphical User Interface
HA	High Availability
I/O	Input/Output
JNDI	Java Naming and Directory Interface
ODBC	Open Database Connectivity
OEM	Original Equipment Manufacturer
OS	Operating System
PPM	Principal Period of Maintenance
PWGSC	Public Works and Government Services Canada
RAID	Redundant Array Of Independent Disks
RFU	Ready for Use
RTM	Release to Market
RTO	Recovery Time Objective
SIEM	Security Information and Event Management
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOR	Statement of Requirements
SQL	Structured Query Language
SQLJ	Structured Query Language Java
SSC	Shared Services Canada
TB	Terabytes
XML	Extensible Markup Language

Appendix 5 Acceptable Use Policy (AUP)

All Contractor personnel accessing DCH, DCSL and/or DCWQ data centres must read, sign and adhere to an Acceptable Use Policy (AUP) which includes the following conditions;

a) The Contractor personnel must only use services supplied by the Contractor for lawful purposes;

b) The Contractor personnel may not transmit, retransmit, redirect, display, or store material in violation of any applicable laws (including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations), industry or community standards. This includes, but is not limited to material that is; obscene, indecent, defamatory, libellous, racist, or threatening;

c) The Contractor personnel may not engage in activity that may or will interfere with the service of another user, host or network;

d) The Contractor personnel may not engage in the distribution of software, programs or messages that may cause damage or annoyance to persons, data, and/or computer systems;

e) The Contractor personnel may not engage in fraudulent activities including, but not limited to, intentional misrepresentations or misleading statements, writings or activities made with the intent that the person receiving it will act upon it; obtaining services with the intent to avoid payment; and hosting of phishing websites;

f) The Contractor personnel is prohibited from activity considered a precursor to attempted security violations including, but not limited to, any form of scanning, probing, or other testing or information gathering activity;

g) The Contractor personnel may not attempt to penetrate security measures of other systems;

h) The Contractor personnel may not attempt unauthorized access including illegal, unauthorized access to, or attempt to access, other computers, accounts, networks or systems;

i) The Contractor personnel may not introduce any prohibited item into the data center (raised floor area). Prohibited items include, but are not limited to, the following:
    - combustible materials (i.e. cardboard or foam);
    - food / drinks, explosives, weapons, hazardous materials, electro-magnetic devices, radioactive materials;
    - alcohol, illegal drugs and other intoxicants;
    - cameras, video and other photographic equipment along with but not limited to audio monitoring, audio capture devices or any other recording device;

j) The Contractor personnel may not take pictures without express written consent by the Data Centre IT Manager;

k) The Contractor personnel may not store any materials in the Client Cage Area (other than equipment manuals);

l) The Contractor personnel may not store any materials in common areas (i.e. hallways or loading dock);

m) The Contractor personnel are prohibited from lifting or moving raised floor tiles or penetrate walls; and

n) The Contractor personnel may not sub-let or otherwise allow usage of its space to other organizations or individuals who are not explicitly named in the Contract or where SSC does not have full legal responsibility.

Date:_____Print Name: _____Signature: _____

Date:_____ Print Name: _____ Signature: _____

Appendix 6 Roles & Responsibilities (R&R)

The following table illustrates the R&R between Canada and the Contractor.

	Canada	Contractor
Hardware Installation	X	X
Hardware Integration	X	X
Hardware Repair		X
Hardware Upgrade		X
Software Patching	X	X
Device Management	X	
Back-up Plan	X	
Capacity Plan	X	
Performance Management	X	
Data Management	X	

Appendix 7 Media Protection Security Control Policy

The following table lists each Media Protection (MP) Security Control (SC) identified in the *ITSDF Security Control Catalogue*, required for systems Designated Protected "B", and describes the measures used by the [Software Category] to implement each SC:

No.	Name	Requirement(s)
MP-1	Media Protection Policy and Procedures	**Control:** (A) Policy: CRA, *Security for the Computing Environment Policy*, MITS, Section 16.1, 16.2 (B) Procedure: (C) Standard: *TBS-OSS - Physical Security*
MP-2	Media Access	**Control:** (A) restrict access to media (B) document media requiring restricted access, individuals authorized, and specific measures to restrict access **Enhancement:** (1) use automated mechanisms to restrict access to media storage areas and to audit access **Related:** MP-4
MP-3	Media Labelling	Tailored **Control:** (A) label removable media and output with distribution limitations, handling caveats, and security (B) exempt [list of media types or hardware] from labelling in [protected environment] (C) documents media requiring labelling and specific measures for protection (D) comply with *TBS Security Organization and Administration Standard*,
MP-4	Media Storage	**Control:** (A) physically protect and securely store media in [controlled area] as per *RCMP G1-001, Security Equipment Guide* (B) physically protects and securely stores protected media awaiting destruction in [controlled areas or containers] as per *RCMP G1-001, Security Equipment Guide* (C) protects media until destroyed or sanitized by procedures as per *CSEC ITSG-06 3293 Cleaning and Declassifying Electronic Data Storage Devices* (D) Protected "A"ssets stored in approved containers listed in *RCMP Guide G1-001, Security Equipment Guide* **Related:** AC-19, CP-5, CP-8 and MP-2
MP-5	Media Transport	**Control:** (A) protects [media types] during transport outside

No.	Name	Requirement(s)
		controlled areas using [security measures] as per *TBS-OSS on Physical Security* and *RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets* (B) maintain accountability for media during transport (C) restricts activities associated with transport of media to authorized personnel (D) ensures disposition of information as per TBS Policy on the Management of Government Information through the following practices: • adhering to departmental retention and disposition plans, the National Archives-Approved Records Disposition Authorities, and other legal and policy obligations to ensure the timely disposition of information that is no longer required by the institution • transferring to the National Archives information designated as having historical value • transferring to the National Library publications declared surplus • considering its transfer to non-federal government Departments, subject to legal and policy obligations **Enhancement:** (1) document activities for media transport using [system of records] as per Departmental risk assessment **Related:** AC-15 and CP-8
MP-6	Media Sanitization and Disposal	**Control:** (A) sanitize media prior to disposal or release for reuse (B) perform disposal of documents, machine-readable media and information technology equipment containing Department information as per RCMP *G1-001, Security Equipment Guide* and CSEC *ITSG-06 Clearing and Declassifying Electronic Data Storage Devices* (C) safeguard information in transit to destruction, in highest level for Protected information as per RCMP *Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets* (D) ensure Protected "A"ssets awaiting destruction, either on- or off-site, are stored in approved security containers or appropriate secure room in accordance with the *RCMP G1-001*

Appendix 8 Security Controls Profile

The **"Solution"** referenced herein is defined in Appendix 3 – Definitions of the Statement of Requirements.

Control (ITSG-33)	Enhancement	Name	Description
AC-2		Account Management	The solution allows for the management of information systems accounts including: (A) identifying account types (i.e.,individual, group, system, application, guest/anonymous, and temporary). (B) establishing conditions for group membership. (C) identifying authorized users of the information system and enabling specification of access privileges. (D) (where possible) providing a mechanism for appropriate approvals for requests to establish accounts. (E) allowing the establishing, activating, modifying, disabling, and removing of accounts.
AC-3		Access Enforcement	The solution provides functionality that enforces approved authorizations for logical access to the system in accordance with applicable policy.
AC-4		Information flow enforcement	The solution enforces approved authorizations for controlling the flow of information within the solution and in accordance with applicable policy must function in an environment where information flow is strictly monitored and enforced.
AC-4	17	Information flow enforcement	The solution allows for : (a) Unique identification and authentication of source and destination domains for information transfer.
AC-5		Separation of duties	The solution allows for: separation of duties of individuals as necessary, to prevent malevolent activity without collusion through configurable assigned information system access authorizations
AC-7		Unsuccessful login attempts	The solution should provide an enforceable configurable limit to automatically lock the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
AC-8		System Use Notification	The solution should provide a configurable method to display an approved system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the TBS Policy on the Use of Electronic Networks and The information system should allow for retention of the notification message or banner on the screen until users take explicit actions to log on to or further access the solution.
AU-3		Content of Audit Records	The solution is capable of producing audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.
AU-5		Response to audit processing failure	The solution should provide functionality that alerts designated organizational officials in the event of an audit processing failure.
AU-6	1	Audit Review Analysis and Reporting	The solution provides audit review, analysis, and reporting processes capabilities to support GC processes for investigation and response to suspicious activities.

Control (ITSG-33)	Enhancement	Name	Description
AU-8		Time Stamps	The solution uses internal system clocks to generate time stamps for audit records.
AU-12		Audit Generation	The solution provides audit record generation capability for the list of auditable events defined in AU-3. (B) The solution allows designated GC personnel to select which auditable events are to be audited by specific components of the system. (C) The solution generates audit records for the list of audited events defined in defined in AU-3.
CA-2		Security Assessments	The GC may employ an independent assessor or assessment team to conduct an assessment of the security controls in the solution.
CA-3		Information System Connections	The Contractor documents, for each connection, the interface characteristics, security control requirements, and the nature of the information communicated.
CM-2		Configuration Management	The Contractor will develop, document, and maintain under configuration control, the current baseline configuration (on delivery) of the solution. A baseline configuration should include all current patches for the operating system and applications installed. The baseline should also deactivate all unused ports, services and software and use an hardened configuration (e.g., guest accounts deactivated, access control to all system files and directories applied, default passwords changed)
CM-3		Configuration Change Control	(A) In preparation for product acceptance with the GC and in consultation with the GC, the Contractor must determine the types of changes to the solution that are configuration controlled. (B) The GC approves configuration-controlled changes to the solution with explicit consideration for security impact analyses. (C) The Contractor documents approved configuration-controlled changes to the solution. (D) The GC retains and reviews records of configuration-controlled changes to the solution. (E) The GC audits activities associated with configuration-controlled changes to the solution. (F) The GC coordinates and provides oversight for configuration change control activities through GC Change Control Procedures.
CM-5		Access Restrictions for Change	The GC defines documents, approves, and enforces physical and logical access restrictions associated with changes to the solution. The Contractor must comply with these restrictions upon contract award.
CM-5	3	Access Restrictions for Change	The solution prevents the installation of software or firmware that are not signed with a certificate that is recognized and approved by the GC.
CM-6		Configuration Settings	(A) In consultation with the GC and until such time as the product is accepted, the Contractor establishes and documents mandatory configuration settings for information technology products employed within the solution using GC operational checklists that reflect the most restrictive mode consistent with operational requirements. (B) The Contractor implements the configuration settings. (C) The Contractor identifies, documents, and seeks approval from

Control (ITSG-33)	Enhancement	Name	Description
			the GC for exceptions from the mandatory configuration settings for individual components within the solution based on explicit operational requirements. (D) After acceptance, the GC monitors and controls changes to the configuration settings in accordance with GC policies and procedures.
CM-7		Least Functionality	In consultation with the GC, the Contractor configures the solution to provide only essential capabilities.
CM-8		Information System Component Inventory	As part of service delivery and until the product is accepted by the GC (A) The Contractor develops, documents, and maintains an inventory of solution components that accurately reflects the original state of the solution. (B) The Contractor develops, documents, and maintains an inventory of solution components that is consistent with the authorization boundary of the information system. (C) The Contractor develops, documents, and maintains an inventory of solution components that is at the level of granularity deemed necessary for tracking and reporting. (D) The Contractor develops, documents, and maintains an inventory of solution that includes: hardware, firmware and software components and versions.
CP-9		Information System Back-up	(A) The solution must allow for configurable backups (based on variable frequency) of user-level information contained in the solution. This is also addressed in the SOR.
CP-10	2	Information System Recovery and Reconstitution	The solution implements transaction recovery for systems that are transaction-based.
CP-10	6	Information System Recovery and Reconstitution	The Contractor provides the capability to re-image solution components within from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.
IA-2		Organizational Users	The solution provides capability to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).
IA-3		Device Identification and Authentication	The solution provides capabilities to uniquely identify and authenticate users and devices before establishing a connection.
IA-3	2	Device Identification and Authentication	The solution should authenticate devices before establishing network connections using bidirectional authentication between devices that is (GC approved) cryptographically based.
IA-5	1	Authenticator Management	The solution, for password-based authentication provides capabilities to: (a) Enforce minimum password complexity of including a minimum of 8 characters with a mix of uppercase, lowercase and special characters; (b) Enforce at least a change of 3 characters when new passwords are created;

Control (ITSG-33)	Enhancement	Name	Description
			(c) Encrypt passwords in storage and in transmission; (d) Enforce password minimum and maximum lifetime restrictions; and (e) Prohibits password reuse for 2 generations.
IA-5	2	Authenticator Management	The solution, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account.
IA-6		Authenticator Feedback	The solution obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
MA-3		Maintenance Tools	The GC will approve, control, monitor the use of, and maintains on an ongoing basis, solution maintenance tools.
MA-4		Non Local Maintenance	(A) The GC authorizes, monitors, and controls non-local maintenance and diagnostic activities.
MA-5		Maintenance Personnel	(A) The GC establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel. (B) The GC ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise solution maintenance when maintenance personnel do not possess the required access authorizations.
MA-6		Timely Maintenance	The Contractor obtains maintenance support and/or spare parts for the required solution components to ensure the RTO requirements as defined in the Statement of Requirements.
PE-7	1,2	Visitor Access Control	The Contractor will comply to the following: GC controls physical access to the solution by authenticating visitors before authorizing access to the facility where the solution resides other than areas designated as publicly accessible. (1) The GC escorts visitors and monitors visitor activity, when required. (2) The GC requires two forms of identification for visitor access to the facility.
PE-16		Delivery and Removal	The Contractor will comply with the following: GC authorizes, monitors, and controlsany of the solutions components entering and exiting the facility and maintains records of those “items.
PL-2		System Security Plan	(A) The Contractor develops a security plan for the information system that: (a) Is consistent with the GC’s enterprise architecture; (b) Explicitly defines the authorization boundary for the solution; (c) Describes the operational context of the information system in terms of missions and business processes;

Control (ITSG-33)	Enhancement	Name	Description
			(d) Provides the security categorization of the solution including supporting rationale; (e) Describes the operational environment for the solution; (f) Describes relationships with or connections to other information systems; (g) Provides an overview of the security control requirements for the solution; (h) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions (including the application of supplemental guidance); and (i) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
SA-4	2	Acquisitions	The GC requires that the Contractor provide information describing the design and implementation details of the security controls to be employed within the solution, solution components, or solution services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.
SA-4	5	Acquisitions	The GC requires in that solution components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.
SA-5		Information System Documentation	(A) The Contractor supplies, protects as required, and makes available to authorized personnel, administrator documentation for the solution that describes: (a) Secure configuration, installation, and operation of the solution; (b) Effective use and maintenance of security features/functions; and (c) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. (B) The Contractor supplies, protects as required, and makes available to authorized personnel, user documentation for the solution that describes: (a) User-accessible security features/functions and how to effectively use those security features/functions; (b) Methods for user interaction with the solution, which enables individuals to use the system in a more secure manner; and (c) User responsibilities in maintaining the security of the information and solution.
SA-7		User Installed Software	The Contractor enforces explicit rules governing the installation of software by users.
SA-12		Supply Chain Protection	The Contractor employs standard configurations for the solution, information system components, and information technology products.
SC-2		Application partitioning	The solution separates user functionality (including user interface services) from solution management functionality.
SC-5	2	Denial of Service Protection	The solution must function in an environment which manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.
SC-6		Resource Priority	The solution limits the use of resources by priority. This is also addressed in the SOR.
SC-7		Boundary Protection	(A) The solution monitors and controls communications at the external boundary of the solution and at key internal boundaries

Control (ITSG-33)	Enhancement	Name	Description
			within the solution. (B) The solution connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
SC-7	5	Boundary Protection	The solution at managed interfaces must function in an environment which denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
SC-7	9	Boundary Protection	The solution, at managed interfaces, must function in an environment which denies network traffic and audits internal users (or malicious code) posing a threat to external information systems.
SC-7	14	Boundary Protection	The solution must function in an environment which protects against unauthorized physical connections across the boundary protections implemented at the GC network.
SC-7	15	Boundary Protection	The solution routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.
SC-8		Transmission Integrity	The solution protects the integrity of transmitted information.
SC-9		Transmission Confidentiality	The solution protects the confidentiality of transmitted information.
SC-13		Use of Cryptography	The solution implements cryptographic mechanisms using cryptographic systems that comply with applicable GC legislation and TBS policies, directives and standards.
SC-13	1	Use of Cryptography	The Contractor on behalf of the GC employs, at a minimum, CMVP-validated cryptography to protect data
SC-23		Session Authenticity	The solution provides mechanisms to protect the authenticity of communications sessions.
SC-28		Protection of Information at Rest	The solution protects the confidentiality and integrity of information at rest.
SI-2		Flaw Remediation	(A) The Contractor identifies, reports, and corrects information system flaws. (B) The Contractor tests software updates related to flaw remediation for effectiveness and potential side effects on GC information systems before installation.
SI-3	5	Malicious Code Protection	The Contractor does not allow users to introduce removable media into the solution
SI-9		Information Input Restrictions	The solution restricts the capability to input information to the information system to authorized personnel.
SI-11		Error Handling	(A) The solution identifies potentially security-relevant error conditions. (B) The solution generates error messages that provide information necessary for corrective actions without revealing protected information in error logs and administrative messages that could be exploited by adversaries. (C) The solution reveals error messages only to authorized personnel.
SI-13		Predictable Failure Prevention	(A) The Contractor protects the solution from harm by considering mean time to failure for solution in specific environments of operation.

Control (ITSG-33)	Enhancement	Name	Description
			(B) The Contractor provides substitute solution components, when needed, and a mechanism to exchange active and standby roles of the components.
SI-13	1	Predictable Failure Prevention	The Contractor takes the solution component out of service by transferring component responsibilities to a substitute component no later than 4 hours for Severity 1 and 24 hours for other queries of mean time to failure.