RCMP
ROYAL CANADIAN MOUNTED POLICE

Systems Delivery and Project Portfolio Management (SDPPM)

AFIS Renewal

APPENDIX A: AFIS RENEWAL STATEMENT OF WORK

Last Updated Date:	2016-06-20
Status:	Final
Version:	2
RDIMS Document No.:	42071v15b

TABLE OF CONTENTS

TABLES

FIGURES

1. INTRODUCTION

1.1 General

1. In order to support planned future biometric processing requirements for Real Time Identification (RTID), the Royal Canadian Mounted Police (RCMP) will require a renewal of the existing Automated Fingerprint Identification System (AFIS) and its related subsystems. This Statement Of Work (SOW), its accompanying annexes and compliancy documents describe the requirements that must be satisfied to renew the AFIS and its related subsystems. (M)
2. In addition to renewing the AFIS and its subsystems, the RCMP has a requirement to expand its processing capacity to support significantly increased fingerprint processing volumes as well as new biometric processing capabilities such as facial recognition. (I)
3. The Contractor shall provide the goods and services described herein in accordance with the terms and conditions of the contract resulting from this SOW that will enable the RCMP to continue efficient, effective and secure AFIS processing for RTID. (M)

1.2 High-level Requirement

1. This requirement includes the renewal of AFIS and its related subsystems with a Commercial Off-The-Shelf (COTS) based solution. This COTS based solution must be configurable to support the AFIS and its related subsystem requirements. The RTID AFIS solution includes all AFIS and Verification Sub-system (VSS) capabilities; as well as AFIS workstations, printers, cameras and scanners used by RCMP staff for all types of fingerprint analysis; and remote Transcoders which are used by major Canadian Police agencies to complete crime scene fingerprint investigations. In addition to renewing all the existing RTID AFIS related capabilities, the Contractor must provide a Latent Case Management Capability (LCMC) and must be able to provide facial recognition capabilities. Therefore, the Entire AFIS renewal solution includes renewing the existing RTID AFIS solution as well as the new AFIS related capabilities required to satisfy all requirements stated in this SOW and its accompanying documents. (M)
2. These requirements shall include the replacement/upgrade/re-use of all components and subsystems in the Production environment and three (3) test environments. (M)
3. The replacement/upgrade/re-use of the test environment hardware, operating system (OS) and software must ensure the test environments can be used to effectively test all Production functionality. (M)
4. This requirement shall include the support and maintenance of all environments in a manner that provides a secure operating environment within the RCMP / Shared Services Canada (SSC) infrastructure. (M)
5. This requirement shall include user training on the User Interfaces (UI) for the entire AFIS renewal solution as well as ongoing support and maintenance of all AFIS components. (M)

6. This requirement also includes the conversion of all data used by the existing RTID AFIS solution. The Contractor must convert the data to a format that is usable by the Contractor's proposed solution. (M)

7. Rated Requirements are marked with "(R)" at the end of a paragraph or an "R" in tables where rated requirements are listed. The wording used to identify these rated requirements is "should", "could" or "may". (I)

8. Mandatory requirements are marked with "(M)" at the end of a paragraph or an "M" in tables where mandatory requirements are listed identified using the terms "must", "shall" or "will". (I)

9. Information items are marked with "(I)" at the end of a paragraph. (I)

1.3 Document Organization

1. This document is organized in a manner that allows the overall high-level requirements to be understood before describing the detailed requirements for each key area to be provided by the Contractor. (I)

2. Unless otherwise stated, all requirements identified throughout this SOW and its annexes, attachments and compliancy documents must be satisfied by the Contractor. (M)

3. The following describes the document organization in point form: (I)

   a. This Appendix A describes the:

      i. Compliancy documents that are key parts to this requirement;

      ii. Scope of supply by the Contractor and the RCMP/SSC;

      iii. High-level RTID architecture in the background section;

      iv. High-level requirements and the key areas to be delivered by the Contractor;

      v. High-level technical requirements to be satisfied by the Contractor's proposed solution;

      vi. On-going support requirements to be provided; and

      vii. All the deliverables that to be completed by the Contractor;

   b. Annex A describes the current RTID/AFIS/VSS architecture;

   c. Annex B describes the detailed requirements for AFIS;

   d. Annex C describes the detailed requirements for Transcoders;

   e. Annex D describes the detailed requirements for VSS;

   f. Annex E describes the detailed requirements for the LCMC;

   g. Annex F lists all Government Furnished Equipment (GFE) available for use by the Contractor; and

h. Annex G lists the workflows for the NNS processing that requires interaction with AFIS.

1.4 Document Purpose

1. The purpose of this SOW is to present the RCMP's functional, technical, management, support and maintenance requirements related to the Entire AFIS renewal requirements to be delivered by the Contractor. (I)

2. The requirements contained in this document and referenced in other attached documents will be used by Canada to select a Contractor to install, configure, make fully operational according to the requirements stated herein and support a renewed RTID AFIS solution. (I)

3. This document provides the requirements that must be supported to enable the RCMP as well as other national and international police agencies to effectively process all types of submissions received by RTID. It details the functional requirements, technical requirements, interface specifications, performance, capacity requirements, quality, security, availability, integrity, training, conversion, implementation, and support requirements that the Contractor must satisfy. (M)

1.5 Compliancy Standards and Reference Documents

1.5.1 DOCUMENTS FORMING PART OF STATEMENT OF WORK

1. The following documents form an integral part of this SOW. The Contractor must propose a solution that complies with the content of all the listed documents in this subsection. (M)

   - AFIS Internal Subsystem Interface Control Documents (a.k.a. AFIS ICDs) (Versions 2.0, 2.1), (RDIMS #42236, 42562);
   - Web Service Transport Description Document (RDIMS #18413);
   - NPS-NIST ICD for Immigration External Contributor (IEC) 2.1.1, (AKA: TRB ICD) (RDIMS #40361);
   - TRB Verification Interface Specification Document, (RDIMS #38553);
   - NPS-NIST ICD 177 for External Contributors, (RDIMS #22062);
   - NPS-NIST ICD 178 for External Contributors, (RDIMS #38923);
   - American National Standards Institute National Institute of Standards and Technology – Information Technology Laboratory ANSI NIST-ITL 1-2011 version as of January 2014 or later. That is, the Contractor's solution must support the 2013 update to the ANSI NIST-ITL 1-2011;
   - Electronic Biometric Transmission Specification (EBTS) V10 (including support for both Extended Feature Set (EFS) and Legacy Integrated Automated Fingerprint Identification System (IAFIS) Type-9); and

- RTID Secure File Transfer Technical Architecture (RDIMS #39435) (provided after non-disclosure agreement signed).

1.5.2 REFERENCE DOCUMENTS

1. The following documents are for reference purposes. The Contractor could use these documents to understand RTID related information. These documents include RTID internal Transaction definitions which are used for paper conversion and for RTID to represent external transactions in an internal form such as Internal Criminal Transaction (CARI), Internal Civil Transaction (MAPI), Internal Refugee Transaction (REFI) and LFSNS. (I)

   - Addendum to AFIS ICD (Versions 2.0), (RDIMS #42237); and
   - Internal Subsystem (IIS) ICD (RDIMS #17261).

1.5.3 MAINTAINABILITY PROCESS

1. The RCMP/SSC has a mature release and change management process. The Contractor must adhere to the RCMP/SSC current change management policy found at (this link is only available on the RCMP's intranet): (M)

   http://infoweb.rcmp-grc.gc.ca/cio/cm-gc/index-eng.htm

2. The RCMP will provide the Contractor with a printed copy of the material found in the above link, upon request. (I)

1.6 Scope of Supply

1. This section outlines the scope of supply for the Contractor and the corresponding supply by the RCMP. This is not intended to be a comprehensive list. This list is intended to provide the Contractor with an understanding of the scope of the requirements without reviewing all documentation included in this SOW to determine their potential interest in responding to this Request for Proposal (RFP). The Contractor must supply all goods and services required to satisfy all the requirements stated in this SOW and its accompanying documents. (M)

1.6.1 THE CONTRACTOR

1.6.1.1 Included in Supply

1. Hardware, OS, software and all other deliverables (excluding GFE) required to renew the AFIS, Transcoders, VSS and LCMC such that they shall satisfy the requirements stated throughout this SOW and its accompanying documents; and comply with server/workstation security requirements of the RCMP for all environments: (M)

   a. Development/Test (DEVTEST);

   b. Quality Control Systest (QCS);

   c. Maintenance/Certification (MAINT);

d. Production (PROD); and

e. Disaster Recovery. (DR)

f. **Note**: Software means any drivers, application, third-party or any other software required by the Contractor to provide a solution that satisfies all the requirements stated throughout the SOW and its accompanying documents.

2. All software and/or hardware changes required to the GFE to support the requirements stated in this SOW and its accompanying documents. The Contractor must describe in detail how the GFE will be utilized in the Contractor's proposed solution. (M)

3. Any peripheral GFE components (i.e. monitors, printers, flat-bed scanners, hand held scanners) that are not reused by the Contractor must be replaced with quantities including at least as many as the existing Production and test environments as defined in Annex F (Note: cameras must be replaced). (M)

4. Testing to ensure all the Contractor functionality shall be fully operational between all Contractor components; and between the Contractor components and the RCMP/RTID components. (M)

5. Performance testing that verifies the Entire AFIS renewal will satisfy all the capacity and performance requirements stated in this SOW and its accompanying documents. (M)

6. Training shall be completed on all UI aspects of all Contractor components. (M)

7. Conversion of all existing AFIS and its subsystems data to a form usable by the Contractor's proposed solution that shall satisfy all requirements in this SOW and its accompanying documents. (M)

8. Management of the Contractor's personnel, tasks and processes that ensures the timely, effective and efficient completion of all work identified in this SOW and its accompanying documents will be completed. (M)

9. All other deliverables and services required by the Contractor that will satisfy the requirements stated in this SOW and its accompanying documents. (M)

1.6.1.2 Contractor Dependencies

1. RTID is a fully operational system based on the ICDs identified in this SOW. The Contractor's solution must fully support the ICDs. RTID is available to test the Contractor's solution based on the ICDs; therefore, there are no RCMP RTID application dependencies to test all existing functionality. (M)

2. Any new functionality that must be supported by the Contractor's solution, such as the LCMC, must adhere to the ICDs and support the requirements in this SOW and its accompanying documents. (M)

3. Any Contractor components or modifications to existing components required to support the requirements must be provided by the Contractor and these new/modified components must successfully pass RCMP Departmental Security Branch (DSB)

Vulnerability Assessments (VA) before they can be connected to the RCMP Network. (M)

4. The Contractor must complete the work included in this SOW and its accompanying documents within a time frame agreed to by the Contractor and RCMP. The RCMP will maintain a project schedule, that includes the activities to be performed by the Contractor, integrated with the activities that must be completed by the RCMP/SSC. However, the renewal of all AFIS, Transcoder, VSS and LCMC capabilities including all AFIS workstation, printers, cameras and scanners must be fully implemented in all test environments and the Production environment within twelve (12) months of contract award unless specifically identified herein. The Production environment includes both the Primary (PR) and Disaster Recovery (DR) sites implementation. Refer to Subsection 1.11 (Timeliness of Deliverables) for additional information concerning scheduling the work to be completed as detailed within this SOW. (M)

1.6.1.3 Contractor Configuration Management Tools and Process

1. The Contractor must use Configuration Management tools and processes to maintain the software and configuration changes completed throughout the life of the contract resulting from this RFP. The tools and processes must be included in the response to this RFP and described to a level of detail that clearly identifies an effective, efficient and proven method to manage the RCMP specific software/configurations constituting the Contractor’s proposed solution. (M)

1.6.1.4 Contractor Documentation

1. The Contractor must provide sufficient detailed design documentation that explains all aspects of the Contractor’s proposed solution and how the design/architecture of the proposed solution satisfies the requirements stated in this SOW and its accompanying documents. The Data Item Description (DID) DO-01 Software and Documentation (Section 15) describes the documentation that must be provided through the contract resulting from this RFP. (M)

2. DO-01 can be used as a guideline for what should be provided by the Contractor in response to this RFP. It is the Contractor’s responsibility to include the documentation, in response to this RFP, required to demonstrate that all requirements are satisfied. The documentation provided will be used by the Government Of Canada (GC) to evaluate the proposed solution. (R)

1.6.1.5 Benchmark Testing

1. At no cost to Canada, benchmark testing must be completed in North America (i.e. Canada or continental USA) at a location proposed by the Contractor and agreed to by the RCMP. (M)

2. The benchmarks will take approximately five (5) days per Contractor with, ideally the fifth day of each Benchmark set aside for data reduction and analysis, re-running of tests (only under exceptional conditions) and any required administrative actions. (I)

3. The Contractor is responsible for providing and configuring a benchmark configuration of the proposed solution to be used in the benchmark testing. (I)

4. The Contractor will be provided with the benchmark data set and the first test must start 30 calendar days from the next business day. (M)

5. The Contractors will submit their detailed Benchmark Procedures to the RTID Public Works and Government Services Canada (PWGSC) Procurement Officer no later than fifteen (15) working days prior the scheduled benchmark. The Contractor's Benchmark Test Procedures will be reviewed by the benchmark evaluation team and feedback will be provided five (5) days prior to the first day of its benchmark. This scheduling and other related details will be discussed further with the Contractor's that successfully reach the benchmark testing stage. (M)

6. If Canada determines during the benchmark test that the Contractor's proposed solution does not meet the mandatory requirements, where the Contractor's proposal stated it would be supported within the scope of the benchmark test of this solicitation, the Contractor's proposal may be declared non-compliant and be disqualified. (I)

7. Canada may, as a result of any such demonstration, reduce the score of the Contractor on the COTS rated requirements, if the benchmark test indicates that the score provided to the Contractor on the basis of its written proposal is not validated by the benchmark; where the Contractor's proposal stated it would be supported within the scope of the benchmark test. This is to ensure a Contractor's score for COTS compliancy is accurately determined. No Contractor's score will be increased as a result of any demonstration during the benchmark. (I)

8. If a Contractor is not ready to commence the execution of the Benchmark tests on its scheduled date and time, the benchmark will be considered a failed benchmark. The only exception for not being ready to start that may be accepted is if there are circumstances outside the control of the Contractor (e.g. acts-of-God, war, terrorism or widespread power outages) in which case PWGSC may establish a revised schedule based on the situation. (I)

1.6.1.6 Exclusions

1. There is no requirement to renew/replace the Paper Conversion Subsystem (PCS) servers or PCS workstations. (I)

1.6.2 RCMP

1.6.2.1 Included in Supply

1. GFE servers and AFIS/Transcoder workstations recently procured by RCMP through a GC National Master Standing Offer (NMSO) and existing Transcoder flatbed scanners. Refer to Annex F which includes all components provided as GFE. (I)

2. Cisco network devices such as Layer three (3) switches and stackable switches. The Layer three (3) switches include Load Balancing (LB) capabilities, Secure Sockets Layer (SSL) termination and synchronous Hypertext Transfer Protocol (HTTP) communication between the RCMP/SSC and the Contractor's VSS solution. (I)

3. Communications Security infrastructure. (I)

4. McAfee ePolicy Orchestrator (ePo) services and McAfee client software as required. (I)
5. Internal/external communications infrastructure. (I)
6. Storage Area Network (SAN) storage. (I)
7. Server room space, hook-ups. (I)
8. RCMP server room racks, as stated in Section 3.3.1 Servers, and server cabling between racks and network switches. (I)
9. Technical support for installation to RCMP/SSC components (e.g. network switches). (I)
10. NPS-NIST Server (NNS) functionality including all interface capabilities based on the ICDs. (I)
11. Project management of the overall project, within which the Contractor activities must be included. The RCMP/SSC has a mature release process which will be followed for the Entire AFIS renewal solution. (I)
12. Coordinating Contractor access to Subject Matter Experts (SMEs). (I)
13. Approval authority for decisions, approvals and sign-off required by Contractor. (I)

1.7 Terminology Clarification

1. The phrase “any OS and/or software upgrade completed through the execution of the work required to complete this SOW must successfully pass a DSB VA” or similar phrases concerning VAs represents a requirement for all networked components to operate with an acceptable level of risk in the RCMP infrastructure. This does not mean that every identified vulnerability must be resolved. However, vulnerabilities must be resolved to an acceptable level for DSB approval. What is considered an acceptable level of risk is defined only by RCMP’s DSB. The names of the tools and applications used by DSB to identify the vulnerabilities can be provided to the Contractor, as required. As well, VAs can be performed as soon as the Contractor has a replacement or upgraded component configured for final delivery to ensure vulnerabilities are identified as early as possible in the implementation process; therefore, enabling corrections as soon as possible. (I)
2. In the context of this SOW, the term “component” means any identifiable part of the Contractor’s solution required to provide a fully operational solution that satisfies all the requirements in this SOW and its accompanying documents. For example, components might include servers, workstations, printers, scanners, cameras, databases, firmware and any other devices/products required to provide the Entire AFIS renewal solution. (I)

1.8 Bilingualism

1. The Contractor’s Entire AFIS renewal solution shall be delivered in Canadian English and Canadian French at the user interface level. The Contractor shall describe how language is implemented architecturally in their solution. (M)

2. English and French should not appear on a screen at the same time but users shall sign in with either one of the two languages. (R)

3. The Contractor's Entire AFIS renewal solution shall be functionally equivalent in both official languages (Canadian English and Canadian French) according to Canadian Federal Government standards. The Entire AFIS renewal solution must adhere to the following Acts and Policies: (M)

    a. Official Languages document entitled *Official Languages Act* at http://laws-lois.justice.gc.ca/eng/acts/O-3.01/; and

    b. The document entitled *Policy on Using the Official Languages on Electronic Networks* at https://www.tbs-sct.gc.ca/archives/hrpubs/ol-lo/uoletoc01-eng.asp.

4. The software shall support accented and special characters for the input of French data, in data fields where this is allowed. (Refer to the NPS NIST External ICDs). (M)

5. The shortcut keys shall reflect the language of the interface being used (e.g. "N" for "Next" would become "S" for "Suivant"). (M)

6. The software shall use Canadian spelling, either Canadian English or Canadian French (e.g. "colour" instead of "color"). (M)

7. The Entire AFIS renewal solution shall permit users to select their default language of operation as part of their profile. (M)

8. The Entire AFIS renewal solution shall use common language-independent codes to ensure that selecting a new description from a code table value, when editing the file in one language, is automatically reflected when the file is viewed/edited in another language. (M)

9. The ICDs in Section 1.5 (Compliancy Standards and Reference Documents) contain the code values that are applicable to each input field. (I)

10. The Entire AFIS renewal solution shall make a French and English description available for each code table value. (M)

11. The Entire AFIS renewal solution shall display the description associated with a code table value in the language currently selected by the user. (M)

12. The values displayed from the code tables do not change with the selected language, but the descriptions of the code table values associated with the selected language must change based on the language. (M)

1.9 Security

1. RTID, AFIS and its subsystems operate in a GC Protected B environment. The Contractor must be experienced operating and supporting an AFIS in a Protected B environment. (M)

2. The software and document deliverables are considered Protected A. The Contractor must be experienced handling Protected A deliverables. Any exchange of software or AFIS related documentation between Contractor resources at RCMP sites and off-site Contractor resources must be exchanged securely through a Contractor provided

secure portal. As well, any exchanges of AFIS related software/documentation between RCMP/SSC resources and off-site Contractor resources must be exchanged through a Contractor provided secure portal. (M)

3. For security reasons, all equipment, except Transcoders, provided by the Contractor must be physically located on RCMP premises and used exclusively by RCMP/SSC and Contractor resources on RCMP premises. Transcoders must only be used on RCMP premises or RCMP approved designated law enforcement agencies with secure connections for RTID communication. (M)

4. Under rare exceptions, a temporary secure connection from a specific Contractor off-site location may be allowed to enable engineering assistance for on-site Contractor resources. The on-site Contractor support resources shall perform all daily activities, troubleshoot and resolve all issues as well as complete all the work required to release new software versions through the release process to Production. Consequently, only under rare exception are off-site Contractor personnel expected to require remote access. Planned engineering effort that cannot be performed by the Contractor's support resources shall require the Contractor's engineering staff to be on-site. (M)

5. RCMP's approved mechanism to support external agency devices such as Transcoders is PC Duo. The Entire AFIS renewal solution must be able to provide support using PC Duo as required. (M)

6. The Contractor must gain and maintain RCMP Enhanced Reliability security clearances for a minimum of two (2) personnel or the Contractor will be deemed non-compliant and the contract may be terminated. (M)

1.10 Constraints

1. This section identifies the constraints related to this SOW. (I)

2. The renewed/replaced technology included in the Contractor's proposed solution must be included in the Contractor's ongoing support and maintenance. That is, once accepted and after the warranty period, the renewed/replaced technology will be included in the support and maintenance activities of the Contractor included in this SOW. (M)

3. The Contractor must understand and follow the RCMP Change Management process including the Service Desk Manager (SDM) process, the installation process and release promotion process through various environments to the Production environment. The change management documentation (1.5.3) and Annex A of this SOW – Current Architecture describe the process that the Contractor must follow. This is the same process currently used for RTID NNS, AFIS, Transcoders and VSS and any other RTID component. This process involves the Contractor creating the required documentation to enable an effective and efficient release, including, but not limited to implementation steps, input to the RTID release implementation plan and installation checklist. (M)

4. RCMP will create the SDM Change Orders (CO), as required, for activities completed for this SOW. The Contractor must create all the information and documentation

required for the CO, as documented under this SOW and the RCMP Change Management process. (M)

5. The Contractor is expected to inform the RCMP of anything that might improve the overall solutions requested in this SOW; and/or the efficiency with which the solutions might be implemented. The RCMP has sole responsibility for deciding to use any suggestions presented by the Contractor. (I)

6. There will be no changes allowed to the existing workflows, unless specifically stated in this SOW or its accompanying documents. The NNS is fully operational and already supports the workflows with a specific sequence of activities. Any ICD changes required to support the Contractor's proposed solution must be identified and approved by RCMP prior to submission of the Contractor's proposal. The only ICD changes that will be considered by the RCMP will be changes concerning the new functionality. It will be the sole responsibility of the RCMP to determine whether the ICD change is considered acceptable. (M)

7. RCMP will be responsible for the racking servers, physically moving racked servers to different racks as required and providing power and network connectivity for the servers. (M)

1.11 Timeliness of Deliverables

1. The Contractor must provide the personnel and resources required to complete all the deliverables according to the agreed to Entire AFIS renewal solution SOW Master Contract Schedule (MCS – DID PM-01). The schedule of deliverables (15.2), included herein, provides estimated time frames within which the initial AFIS renewal implementation must be completed. The Contractor must receive written approval from the RCMP, prior to submitting its proposal, to exceed the initial AFIS renewal implementation completion time or the proposal may be considered non-compliant. Any additional time allowed for the Contractor will be communicated to all potential Contractors. (M)

2. The timely completion of all deliverables associated with this SOW is of critical importance to the RCMP. The Contractor must provide highly qualified and experienced resources to ensure the timely completion of all deliverables. (M)

3. All deliverables shall be completed in a timely manner such that they follow all the required review, update, acceptance and approval processes for final sign-off of fully operational solutions according to the MCS. The exception to this date is the ongoing OS and software upgrade activities which must be provided following the completion of all other work in this SOW until the end of the contract resulting from this RFP including any option years that are exercised by the RCMP. (M)

4. All document deliverables provided to RCMP resulting from this SOW will be considered draft until RCMP's acceptance. The RCMP review and approval period for each deliverable is identified in the Section 15, Overall Deliverables Plan and Schedule. (M)

2. BACKGROUND

2.1 General

1. RTID is the Canadian Criminal Real Time Identification Services (CCRTIS) solution to maintain the national repository for criminal, refugee, immigration (aka TRB) and RCMP employee fingerprints. RTID supports submissions from various police agencies, government departments, civil clearance organizations and international police agencies to perform criminal record checks. RTID supports extensive latent crime scene print processing for RCMP Head Quarters' (HQ) staff and personnel from major police agencies across Canada. RTID also supports receiving updates to the criminal and immigration records. Additionally, RTID also supports immigration verification checks at Canadian Ports Of Entry (POE) to verify the identity of an individual seeking entry to Canada. (I)

2. AFIS and its related subsystems provide critical capabilities within RTID. The interface between AFIS related components and RTID is defined through Interface Control Documents (ICDs). (I)

3. The following diagram depicts a high-level view of AFIS and its related subsystems within the current RTID architecture. Annex A describes additional details concerning the current RTID/AFIS/VSS architecture. (I)

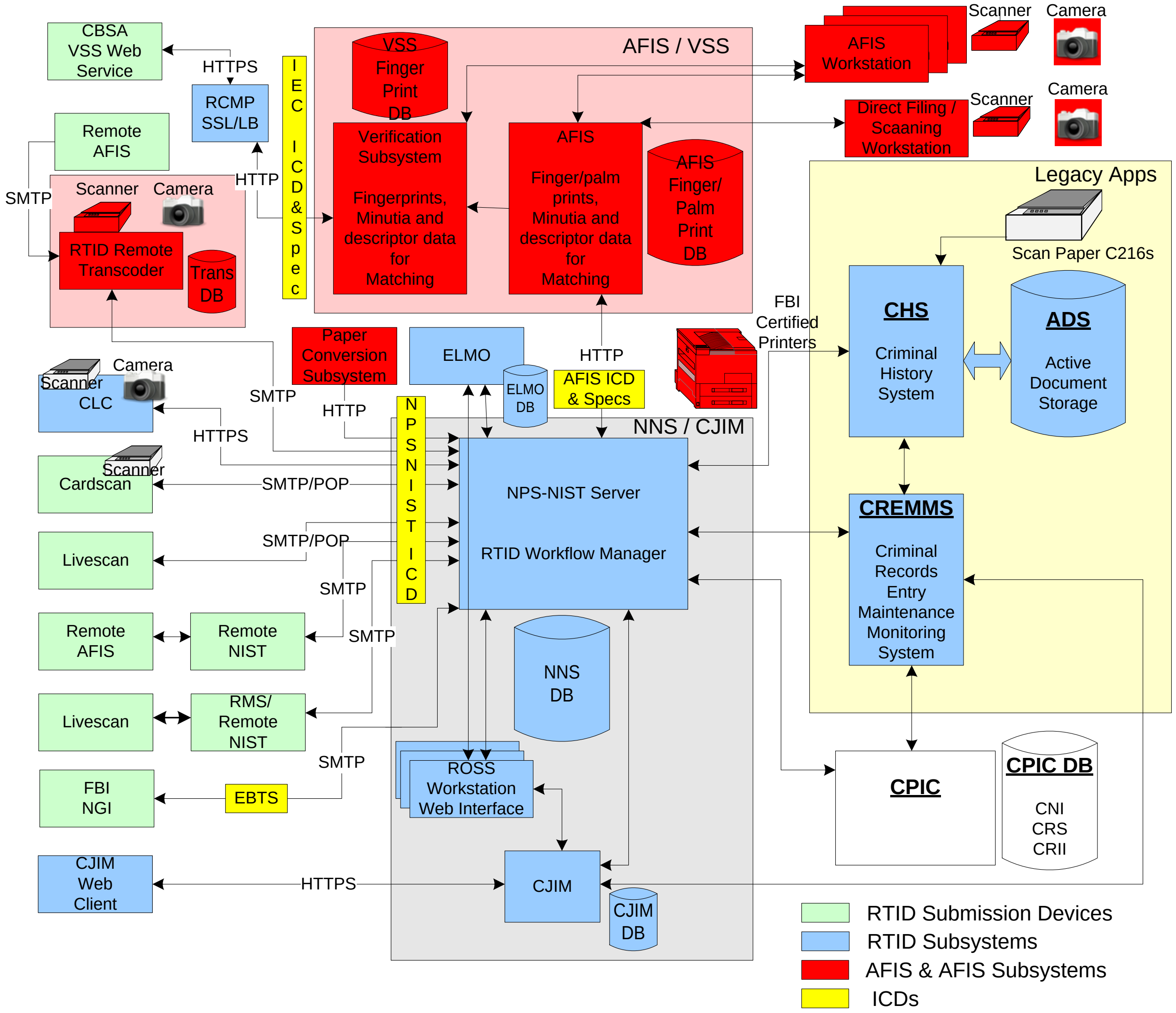

Figure 2-1: Current High- Level RTID Architecture

4. The following is a high-level description of the devices and subsystems depicted in the current high-level RTID architecture diagram: (I)

   a. RTID submission devices:

      i. CardScan, Livescans, remote NIST servers and Records Management Systems (RMS) submit to RTID based on the NPS-NIST ICD 1.7.7/1.7.8 or the NPS-NIST ICD for IEC 2.1.1 for External Contributors. These submission devices might be owned and operated by external agencies or the RCMP. For example the RCMP has a separate NMSO contract that enables the procurement of Livescan and CardScan devices. These devices all submit to RTID using Simple Mail Transfer Protocol (SMTP) and receive responses through either SMTP or Post Office Protocol (POP) email protocols;

      ii. The Canada Border Services Agency (CBSA) VSS web service submits to RTID based on the NPS-NIST ICD for IEC 2.1.1 for External Contributors and the TRB Verification Interface Specification (refer to 1.5 for details). This VSS web service is owned and operated by CBSA. This VSS web service establishes a system-to-system connection with RTID through an SSL session and “posts” NIST packets based on the NPS-NIST ICD for IEC 2.1.1 for External Contributors. The SSL session is through a secure connection provided by the RCMP/SSC; therefore, there is double encryption;

iii. The Central Latent Client (CLC) allows RCMP detachments to submit latent images to RTID based on the IIS ICD. These latent images are processed on AFIS by latent fingerprint analysts specializing in fingerprint crime scene investigation. CLC can also be used to retrieve fingerprint/criminal record information based on the NPS-NIST ICD; and

iv. RTID submission devices are located across Canada and internationally. These devices connect to RTID through a secure connection established between the RCMP/SSC and the contributing agency.

b. RTID subsystems:

i. The NNS is the RTID workflow manager which acts as the hub for almost all RTID activity. The NNS validates all incoming NIST packets to ensure they adhere to the various RTID ICDs and supports communication between most RTID subsystems as depicted in the high-level RTID architecture diagram. The UI for NNS is accessed through a secure portal using the RCMP/SSC RCMP Office Support System (ROSS) workstation from RCMP premises;

ii. Electronic Latent Management Operations (ELMO) is the RCMP Latent case management system which works interactively with NNS to support the CLC Latent submissions. The ELMO UI operates on the RCMP/SSC ROSS workstation with access to the ELMO database on a RCMP/SSC Structured Query Language (SQL) server and includes a few capabilities that are supported through an interface with NNS. The CLC/ELMO/NNS/AFIS processing is typically referred to as Central Latent processing since the fingerprint analysis is completed centrally at RCMP HQ;

iii. The legacy application Criminal History System (CHS) and Active Document Storage (ADS) maintain criminal record related information processed by or relevant to RTID operations. The Criminal Records Entry Maintenance and Monitoring System (CREMMS) is an entry system used to maintain criminal record information maintained on Canadian Police Information Center (CPIC);

iv. The RCMP/SSC Cisco LB/SSL is a module in a Cisco layer three (3) switch that supports SSL establishment with client authentication for the CBSA VSS web interface as well as load balancing and a number of other capabilities;

v. The Criminal Justice Information Modernization (CJIM) system and its CJIM web client provide a mechanism to process dispositions associated with criminal charges previously processed through RTID; and

vi. These RTID subsystems are located at two (2) Data Centers in Canada. The security architecture for these subsystems is provided by the RCMP/SSC.

c. AFIS and Its Subsystems:

i. AFIS is the automated fingerprint processing capability of RTID. Transactions between AFIS and the NNS are based on the AFIS Internal Subsystem ICDs (refer to 1.5 for details);

ii. AFIS workstations interface directly with AFIS to support all AFIS related user activity;

iii. The remote Transcoders are also RTID submission devices; however, they are part of the AFIS solution. The remote transcoders submit to RTID based on the NPS-NIST ICDs 1.7.7/1.7.8 (refer to 1.5 for details). With a few exceptions, the transcoders are owned and managed by the RCMP. A few sites procured additional transcoders that operate as secondary input devices through the primary Transcoder. RTID only interfaces with one RCMP owned Transcoder per site. The Transcoders submit to and receive from RTID using SMTP. The transcoders are based on an AFIS workstation with features specifically supporting latent fingerprint analysis. Essentially Transcoders are remote AFIS workstations with an ability to interface with NNS. The Transcoder operators are non-RCMP police agency Latent fingerprint analysts specializing in fingerprint / palm prints crime scene investigation. Similar to CardScans, Transcoders can also be used to perform criminal records searches using an individual’s fingerprints and retrieve fingerprints records based on the NPS-NIST ICDs 1.7.7/1.7.8. The Transcoder must also support receiving fingerprints / palm prints directly from a remote AFIS to allow larger police agencies to use the Transcoder to search the RTID database if they cannot identify the latent prints against their own agency AFIS database. The RCMP Remote Network Search Coordinators (RNSC) use Transcoders to assist non-RCMP police agencies with coaching and use of the Transcoders through interactive remote sessions using PC Duo. The Transcoder/NNS/AFIS/ELMO processing is typically referred to as Remote Latent processing since the fingerprint / palm print analysis is completed remotely at police agency sites. Confirmed reverse search idents from Remote Latent processing are recorded in ELMO by the RNSC staff. The police agencies are responsible for case management of the Latents they process. The police agencies do not have access to ELMO. Note that with the LCMC solution as part of this RFP, all remote site idents will be recorded automatically (refer to LCMC requirements); and

iv. The VSS is used to verify the identity of a foreign national attempting to enter Canada. Fingerprints of the foreign national received through RTID, prior to the individual’s arrival, are used to compare against CBSA POE fingerprints captured when the individual arrives in Canada. This is a 1:1 search using the immigration identification number provided to the individual when their request to enter Canada was processed by RTID. The VSS performs validation of the received packet against the NPS-NIST ICD for IEC 2.1.1 for External Contributors and a 1:1 search against the previously provided fingerprints of the individual attempting to gain entry to Canada. Performance is a critical requirement for the VSS. The current end-to-end response time is under four (4) seconds; where end-to-end is defined as the moment the CBSA web service starts to send the first byte of data to establish an SSL session with the RCMP LB/SSL module. This sub-four (4) second response time includes any latency on the CBSA connection with the RCMP. The VSS portion of the processing is under three (3) seconds (typically 2.5 seconds) between the RCMP LB/SSL and VSS. This sub-three (3) second response time is measured from the time the LB/SSL sends to VSS and when the LB/SSL receives the complete response from VSS;

v. The AFIS PCS is currently being phased out and will be decommissioned prior to expected delivery date of this AFIS renewal. It is currently used to process paper submissions sent to RCMP. It should not be considered in the response to this SOW;

vi. The AFIS printers used by RTID are Federal Bureau of Investigation (FBI) certified printers;

vii. The Scanners used by Transcoders and direct filing/scanning AFIS workstations to capture images that can be submitted to RTID are FBI certified;

viii. Cameras and hand held barcode scanners are used by AFIS workstations to scan Document Control Numbers (DCNs) / DOCIDs to retrieve fingerprint images and certify a paper submission; and

ix. AFIS and the AFIS subsystems are located at two (2) Data Centers in Canada. The security architecture for AFIS and these subsystems is provided by the RCMP/SSC.

x. Note: Transcoder sites use separate cameras, not included in the scope of this SOW which are used to capture latent images. These images are manually transferred to the Transcoder before a submission is sent.

3. REQUIREMENT

3.1 General

1. The following sub-sections describe the high-level requirements that must be satisfied by the AFIS renewal solution. The detailed requirements for each key area to be delivered are described in the annexes attached to this SOW. (M)

2. The Contractor must provide all the Contractor software, OS, third-party software, configuration and anything else required to create fully operational Production and test environment solutions that function as stated in this SOW and its accompanying documents. (M)

3.2 Key Areas to be Delivered

1. The four (4) key areas that must be delivered by the Contractor under this SOW are AFIS, Transcoders, VSS and LCMC (replacing ELMO). The Contractor's solution must operate effectively in the current RTID security architecture which was presented at the AFIS Renewal Request For Information (RFI) Industry Day December 14–16, 2015. This same information can be provided at RCMP HQ, upon request, after a non-disclosure agreement is signed for anyone that did not attend the Industry Day presentation. The Security architecture will not be presented in this SOW. Only a high-level description of the Security architecture is included in this SOW to provide sufficient information that allows the Contractor to determine their interest and ability to respond to this SOW. Any potential AFIS Contractor would be expected to only need the level of security architecture provided herein to submit a proposal. The Contractor must also provide training and on-going support for all the key areas. (M)

2. The Contractor's solution must be capable of providing facial recognition capabilities that can be integrated into the Contractor's proposed AFIS solution. This integrated facial recognition capability must operate effectively in the current RTID security architecture when/if it is implemented. (M)

3. Additionally, the Contractor must convert all the AFIS, Transcoder, VSS and ELMO data to a form usable by the Contractor's Entire AFIS renewal solution. (M)

4. The Contractor's proposed Entire AFIS renewal solution must support everything in the current architecture, Annex A. That is, the RCMP security/network architecture will not be altered to support an inefficient or less secure AFIS/Transcoder/VSS/LCMC design. The proposed AFIS/Transcoder/VSS/LCMC solution must be able to replace the existing solution. This ability to replace any AFIS related component, based on the ICDs, is a fundamental design concept for RTID. The AFIS renewal solution must meet the requirements stated in this SOW and its accompanying documents based on the RCMP infrastructure already in place which is detailed in the SOW. (M)

5. If the AFIS renewal uses different internal ports within the existing security/network architecture, it would be considered an acceptable difference providing it shall not create a vulnerability that is unacceptable to RCMP's DSB. RCMP is solely responsible for determining whether any aspect of the Contractor's proposed solution creates a vulnerability. (M)

6. As part of maintaining RCMP systems, all of the AFIS/Transcoder workstations and several AFIS servers have recently been replaced using Government Of Canada (GC) National Master Standing Offers (NMSOs). (I)

7. These workstations and servers are considered GFE for this AFIS renewal SOW and they are listed in Annex F. (I)

8. The GFE AFIS/Transcoder workstations use the Windows 7 OS and the Contractor's proposed UI for the AFIS/Transcoder fingerprint analyst must operate on these workstations with Windows 7 or Windows 10 desktop OS. (M)

9. Although not mandatory to utilize the GFE servers, they are available to implement the Contractor's solution. (I)

10. Any costs associated with additional servers; or upgrading the GFE servers or workstations to satisfy the technical, functional or performance requirements of this SOW will be solely the responsibility of the Contractor and must be identified in the Contractor's proposal. As well, the Contractor's proposal must explain how the GFE will be used together with the Contractor's components. The RCMP must approve any changes or upgrades to any GFE components. Any new or modified servers or workstations must successfully pass DSB approval or the proposal would be considered non-compliant. Any proposed changes can be submitted for approval prior to the closing time of the RFP. (M)

11. The Contractor will be responsible for the support and maintenance of the AFIS/Transcoder/VSS/LCMC related GFE including coordinating replacement parts/upgrades from the hardware / operating system vendor under the NMSO support contract. The existing RTID AFIS vendor is currently performing this task, using the onsite support personnel, as part of the terms of the existing contract. Support details will be presented later in this SOW. The Contractor will also be responsible for the support and maintenance of any new components provided to satisfy the requirements in this SOW. (M)

12. The following diagram depicts a high-level view of AFIS and its related subsystems that must be included with the Entire AFIS renewal solution. The notable differences from the current RTID architecture are the replacement of the existing RCMP ELMO case management system and the removal of PCS. This Entire AFIS renewal must include a LCMC that will replace the existing ELMO. The following subsections briefly describe each key area of the Entire AFIS renewal solution that must to be delivered by the Contractor under this SOW. Detailed requirements for each key area are identified in separate annexes attached to this SOW. (M)

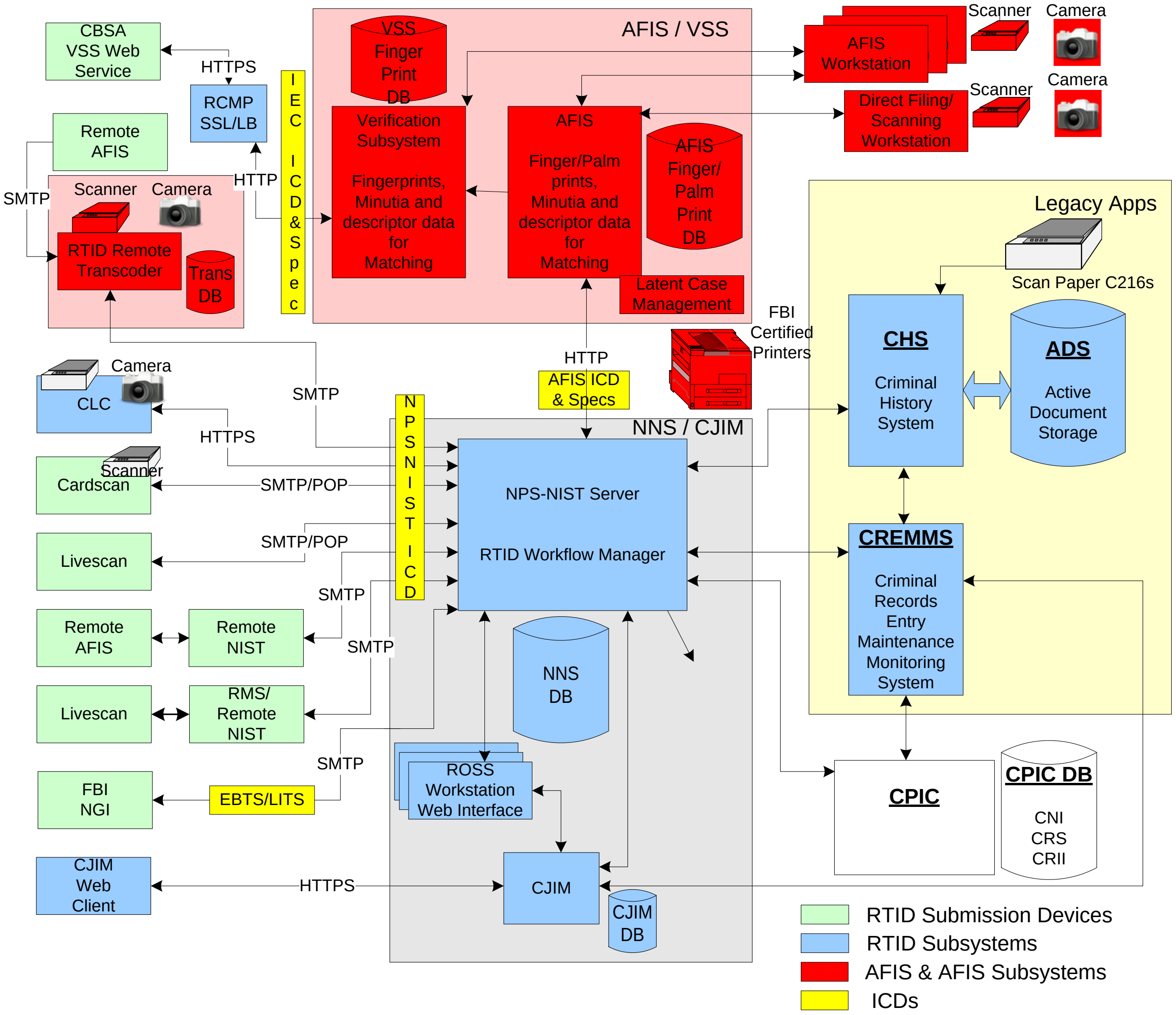

Figure 3-1: Entire AFIS Renewal High-level RTID Architecture

3.2.1 AFIS PRODUCTION AND THREE TEST ENVIRONMENT RENEWAL

1. The AFIS renewal solution must include the following: (M)

   a. Servers, workstations and scanners to support all requirements stated in this SOW for the production environment and three (3) test environments;

   b. Database conversion from the existing AFIS database to the Contractor’s database;

   c. A direct filing and direct scanning capability to support special requirements where a set of prints needs to be filed directly to AFIS;

   d. Support an electronic sync filing capability using AFIS ICD transactions, as required, where the Contractor’s AFIS must support receiving electronic transactions from NNS and processing them completely without responding back to NNS. This will allow two (2) AFIS solutions to operate in parallel until the final cut-over without affecting existing RTID Production operations;

e. FBI certified printers;

f. Cameras to support paper certification and other requirements as stated in this SOW and its accompanying documents; and

g. Anything else required to fully satisfy the requirements stated in this SOW and its accompanying documents.

2. The Production AFIS must operate in RCMP's two (2) Data Center configuration that allows fail-over from RCMP's PR site to the DR site. The AFIS renewal solution must be fully operational, with fifty percent (50%) capacity, at the DR site within eight (8) hours. Refer to Annex A for details concerning the architecture within which the AFIS renewal solution must effectively operate when a site fail-over occurs, as well as the other fail-over requirements as stated in this SOW and its accompanying documents. (M)

3. The test environment servers must be configured in the same, or similar, manner as the Production environment. That is, these servers must be able to support the same OS, software, Database (DB) and configuration that operate in the Production environment which will allow all the Contractor AFIS capabilities to be effectively tested as well as allow Production issues to be recreated in the test environment. Refer to Annex A for details concerning how each test environment must be used and the capabilities that must exist in the test environments. (M)

4. The Contractor shall be responsible for providing the required software necessary to satisfy all the requirements identified in this SOW and configuring the servers with a DSB approved operating environment that will successfully pass the DSB Vulnerability Assessment (VA). (M)

5. The Contractor shall be responsible for providing the required software necessary to satisfy all the requirements identified in this SOW and configuring the GFE AFIS workstations with a DSB approved operating environment that will successfully pass the DSB VA. (M)

6. All production and test environment servers must be maintained with the latest updates for the OS; and the latest Anti-Virus (AV) DAT files and AV policies. For any Windows servers, the maintenance of the latest updates must be through RCMP's automated Windows Server Update Services (WSUS) and McAfee ePolicy Orchestrator (ePo). The Contractor solution must interface with and automatically process data received from RCMP's WSUS and ePo or use manual intervention to complete the updates within five (5) days of receiving the latest Windows patches, DAT files or AV policies. All non-Windows servers must be maintained using either automated or manual processes based on RCMP required security patches and AV DAT files and polices within five (5) days of receiving the data or patch information from the RCMP. (M)

7. All production and test environment AFIS workstations must be maintained with the latest updates for the existing OS and the latest AV DAT files and AV policies. The maintenance of the latest updates must be through RCMP's automated WSUS and

ePo. The Contractor solution must interface with and automatically process data received from RCMP's WSUS and ePo with no manual intervention required. (M)

8. Note: The name and version of the tools used to perform the VAs can be provided upon request. (I)

3.2.2 TRANSCODER RENEWAL

1. The Transcoder renewal must include Transcoder software, workstations and scanners to support all requirements stated in this SOW for the production environment and three (3) test environments. (M)

2. The Transcoder is essentially an AFIS workstation which has been distributed remotely, across Canada, to non-RCMP police agencies. The Transcoder allows non-RCMP police agencies to use the RTID database to perform almost all activities available to an RCMP latent fingerprint analyst that uses an AFIS workstation. (I)

3. The Transcoder must interface with RTID using the NPS-NIST ICDs and communicate with RTID through bi-directional SMTP over a secure communication link. (M)

4. The Transcoder UI must be the same or very similar to the AFIS workstations and it must allow the non-RCMP police agency fingerprint analysts to process crime scene prints independent of the RCMP staff. (M)

5. The Transcoders must provide: (M)

   a. The required functionality as stated in this SOW and its annexes;

   b. A scanner for scanning Latents; and

   c. Allow Latents captured using images from police agency cameras to be submitted to RTID.

6. The Transcoder must also be capable of receiving IAFIS Type-9 records according to the Electronic Biometric Transmission Specification (EBTS) format. In RTID terms, this is referred to as the back-end interface to the Transcoder where larger police agencies send submissions to the Transcoder. These back-end submissions must be automatically received by the Transcoder, automatically converted from a Type-9 record into a latent search and automatically submitted to RTID according to the NPS-NIST ICD. These larger police agencies have their own AFIS and typically only send Latents to RTID that have not been resolved on their own AFIS. (M)

7. The police agencies use SMTP to communicate with the Transcoder back-end interface. The Transcoder must support police agencies submitting IAFIS Type-9 records using SMTP. Responding to the police agency back-end interface is not required. This is a one–way communication; however, the Transcoder mail service must support the SMTP protocol including acknowledging receipt of the email to ensure the police agency's SMTP server receives an acknowledgement that the email was successfully received (i.e. smtp ok 250). (M)

8. The Transcoder must support bi-directional SMTP between the Transcoder and RTID. (M)

9. The Contractor’s solution must include the database conversion from the existing Transcoder database to the Contractor’s Transcoder database. (M)
10. The Contractor shall be responsible for providing the required software necessary to satisfy all the requirements identified in this SOW and configuring the GFE Transcoders with a DSB approved operating environment that will successfully pass a DSB VA. (M)
11. All production and test environment Transcoders must be maintained with the latest updates for the OS and the latest AV DAT files and AV policies. The maintenance of the latest updates must be through RCMP’s automated WSUS and ePo. The Contractor solution must interface with and automatically process data received from RCMP’s WSUS and ePo with no manual intervention required. (M)

3.2.3 VERIFICATION PRODUCTION SUBSYSTEM AND THREE TEST ENVIRONMENT RENEWAL

1. The Verification Subsystem is dedicated to providing real-time one-to-one (1:1) matching in support of biometric verification of a foreign national’s fingerprints received from a CBSA POE to validate an individual’s identity. (I)
2. The VSS renewal must include all the servers to support all requirements stated in this SOW for the production environment and three (3) test environments. (M)
3. The Contractor’s solution must include the database conversion from the existing VSS database to the Contractor’s VSS database. (M)
4. The VSS must be able to operate independently from the AFIS. (M)
5. The Contractor’s solution must include reconciliation/synchronization reporting that verifies consistency between VSS sites; and between the VSS and AFIS on at least a weekly basis. (M)
6. The Production VSS must operate in a dual Data Center configuration that allows automatic use of RCMP’s DR site if the PR site fails. The Production VSS must have at least two (2) nodes per site to ensure the VSS provide intra-site and inter-site High Availability (HA) capabilities. Refer to Annex A for details concerning the architecture within which the renewal AFIS must effectively operate when a site fail-over occurs as well as the other fail-over requirements as stated in this SOW and its accompanying documents. (M)
7. The test environment servers must be configured in the same, or similar, manner as the Production environment. That is, these servers must be able to support the same OS, software, Data Base (DB) and configuration that operate in the Production environment which will allow all the Contractor VSS capabilities to be effectively tested as well as allow Production issues to be recreated in the test environment. Refer to Annex A for details concerning how each test environment must be used and the capabilities that must exist in the test environments. (M)
8. The Contractor shall be responsible for providing the required software necessary to satisfy all the requirements identified in this SOW and configuring the VSS servers with a DSB approved operating environment that will successfully pass the DSB Vulnerability Assessment (VA). (M)

9. The Contractor shall be responsible for providing the required software necessary to satisfy all the requirements identified in this SOW and configuring the GFE AFIS workstations to support the VSS UI in a DSB approved operating environment that will successfully pass the DSB VA. (M)

10. All production and test environment servers must be maintained with the latest updates for the existing OS; and the latest AV DAT files and AV policies. For any Windows servers, the maintenance of the latest updates must be through RCMP's automated WSUS and McAfee ePolicy Orchestrator (ePo). The Contractor solution must interface with and automatically process data received from RCMP's WSUS and ePo or use manual intervention to complete the updates within five (5) days of receiving the latest Windows patches, DAT files or AV policies. All non-Windows servers must be maintained using either automated or manual processes based on RCMP required security patches and AV DAT files and polices within five (5) days of receiving the data or patch information from the RCMP. (M)

3.2.4 LATENT CASE MANAGEMENT CAPABILITY (LCMC) (ELMO REPLACEMENT)

1. The Contractor must provide a fully operational LCMC. This LCMC must be an integrated solution with the Contractor's AFIS. That is, the LCMC/AFIS users must be able to seamlessly interface between the LCMC and AFIS to send fingerprints for search from the LCMC and perform all other required capabilities stated in this SOW. (M)

2. The LCMC and AFIS users are the same users that must use the same AFIS windows workstation to perform either LCMC or AFIS activities. Performing latent case management activities are part of the daily activities for an AFIS Latent Fingerprint Analyst. (M)

3. The preferred LCMC solution is an integrated capability within the AFIS. This would provide a consistent UI for the LCMC/AFIS users and ensure there is no duplication of capabilities available in the LCMC and AFIS. (R)

4. The Contractor's solution must include the database conversion from the existing ELMO SQL database to the Contractor's LCMC database. (M)

5. The LCMC must interface with RTID's NNS using the AFIS ICD. The existing AFIS ICD includes existing transactions that are used to communicate between NNS and AFIS. Some of these existing AFIS ICD transactions were modified for this SOW to enable the communication of latent case management information to be exchanged between NNS and AFIS/LCMC. (M)

3.2.5 TRAINING

1. The Contractor must provide training on all user aspects of the Contractor's proposed Entire AFIS renewal solution. As a minimum this training must include: (M)

   a. AFIS TP and Latent UI;

   b. Transcoder UI;

   c. VSS UI;

d. LCMC UI;

e. Direct filing and direct scanning;

f. All reporting capabilities for all UIs; and

g. All reporting for reconciliation/synchronization processing.

2. Section 10 describes the detailed training requirements that must be satisfied by the Contractor. (M)

3.2.6 ONGOING SUPPORT

1. The Contractor must provide at least one (1) permanent on-site resource at RCMP HQ in Ottawa, Canada. (M)

2. This resource must be available on-site during RCMP core hours (weekdays 8am-5pm eastern time). (M)

3. The Contractor on-site resource must: (M)

   a. Support all AFIS/Transcoder/VSS/LCMC servers, workstations, processes and any other components necessary for the effective and efficient operation of the AFIS and its subsystems;

   b. Be able to support the Production environment and all test environments with minimal assistance from off-site Contractor personnel. This is to ensure the timely resolution of any issues arising in any environment;

   c. Be available between 0600 and 2200, seven (7) days a week including statutory holidays for on-call support for Production related issues;

   d. Ensure that exceptional situations such as vacations, appointments or illness are coordinated in a manner that there is at least one (1) Contractor resource available on-site to support the AFIS environments during RCMP core hours. This requirement indicates that the Contractor must have a backup resource, cleared to Enhanced Reliability, to perform all on-site responsibilities;

   e. Have one (1) hour response time for production or test environment issues during on-site hours;

   f. Have two (2) hour response time from initial notice by the RCMP of a production or test environment issue, during off hours;

   g. Unlimited telephone software and hardware maintenance and support services; and

   h. Provide a strategy and plan to implement a patching regime compliant to RCMP and Government of Canada (GC) standards to maintain all the AFIS/Transcoder/VSS/LCMC servers and workstations at a level that effectively mitigates any risks to an acceptable level. Section 11 describes the detailed on-going patching regime requirements that must be satisfied by the Contractor.

4. The Contractor must provide an English technical toll-free hotline 24 hours per day, seven (7) days a week and 365 days a year. The toll-free number must be provided

within fifteen (15) days of contract award. The Contractor's hotline must be staffed by qualified resources who are able to respond to questions, resolve problems and provide advice regarding problems related to all deliverables as well as installation and integration issues within the Contractor's AFIS/Transcoder/VSS/LCMC solution installed at RCMP. (M)

3.2.7 FACIAL RECOGNITION CAPABILITY (FRC)

1. The Contractor must support a Facial Recognition Capability (FRC) that can be integrated into the Contractor's proposed AFIS renewal solution. (M)
2. This FRC is not to be implemented with the scope of the initial procurement of the AFIS renewal. The FRC is considered a future requirement that might be implemented after the mandatory requirements in the AFIS renewal solution have been implemented. (I)
3. Section 12 describes the detailed FRC requirements that might be described by the Contractor at the time of the Contractor bid submission. (I)

3.2.8 CONVERSION

1. The Contractor must convert all data used by AFIS and its subsystems to a format that is usable by the Contractor's proposed solution. (M)
2. The conversion must be completed on RCMP premises within the RCMP/SSC security architecture. (M)
3. The Contractor must provide a high-level plan and strategy with its proposal explaining: (M)
   a. How the conversion will be completed;
   b. What tools and/or processes will be used to complete the conversion;
   c. When the conversion will be completed; and
   d. Any impact to the existing AFIS data or data format.
4. Section 13 describes the detailed conversion requirements that must be satisfied by the Contractor. (M)

3.3 Hardware and Software

1. All non-GFE hardware proposed by the Contractor must satisfy the requirements stated in this subsection, its subsections and all the other requirements stated throughout this SOW and its accompanying documents. (M)
2. This hardware subsection is broken down into the following subcategories: (I)
   a. Servers;
   b. Scanners;
   c. Printers;

d. SAN Storage; and

e. Cameras.

3. To substantiate the hardware and software requirements below, the Contractor shall provide in its solution a description of the hardware and software and their interrelationship within each environment (production and test environments) including, as a minimum, for each COTS hardware and software component included as part of the technical design: (M)

   a. Item make, model and version number;

   b. The ANSI/NIST compliance and other standards met;

   c. Certifications and ratings achieved;

   d. Number of each required;

   e. Customization required;

   f. Recommended and minimum performance criteria and capacities;

   g. The internal/external electronic interfaces; and

   h. The security services implemented.

4. All Contractor proposed hardware must satisfy RCMP electrical specifications, including the voltage, amperage, electrical receptacle, and Underwriters' Laboratories (UL) or Canadian Standards Association (CSA) certification. (M)

3.3.1 SERVERS

1. The Contractor's AFIS renewal solution shall comply with the following hardware requirements and policies currently implemented within the RCMP: (M)

   a. All AFIS/VSS/LCMC renewal solution servers shall be configurable to operate in a HA clustered environment.

   b. All AFIS/VSS/LCMC renewal solution servers shall support graceful shutdown, such that all "inflight" transactions can be completed or re-started automatically upon server re-start with no loss of data.

   c. All AFIS/VSS/LCMC renewal solution servers shall support automatic restart.

2. The AFIS/VSS/LCMC renewal solution server hardware shall include the following: (M)

   a. Support for multiple Central Processing Unit (CPU) engines;

   b. Support for one (1) Gbps Ethernet connections according to the specifications in Annex B subsection 8.7.1;

   c. Support for server temperature sensor and alarm capability when the temperature of the server becomes too high; and

d. Support for electrical power sensor and alarm capability when the power signature becomes out of specification.

3. All AFIS/VSS/LCMC renewal solution servers requiring access to the RCMP SAN shall be configured to interface to the SAN using multiple Host Bus Adapters (HBAs) each capable of four (4) Gbps. (M)

4. Fiber channel connections are limited and expensive; therefore, the preferred AFIS/VSS/LCMC renewal solution would satisfy all the requirements stated in this SOW and its accompanying documents with a minimum number of fiber channel connections. (R)

5. The Contractor's AFIS/VSS/LCMC proposed solution must have sixteen (16) or less fiber channel connections (i.e. a maximum of eight (8) servers each with two (2) fiber channel connections each) per site unless approved by the RCMP in writing prior to proposal submission. (M)

6. AFIS renewal solution servers to be installed at the RCMP Data Centre or DR site should be compatible with the 19" rack standard (EIA 310-D). If the Contractor provides equipment compatible with the 19" rack standard, then the Contractor is not required to supply racks. RCMP-supplied racks or cabinets will be used. (R)

7. If the Contractor is not proposing standard 19” racks, the Contractor must provide racks at the Contractor's expense which must be included in the Contractor's proposal and must be approved by the RCMP in writing prior to the proposal submission. (M)

3.3.2 SCANNERS

1. Flat-bed Scanners provided with the AFIS/VSS/LCMC/Transcoder renewal solution shall meet, at a minimum, the Image Quality Specification (IQS) of Appendix F in the Electronic Biometric Transmission Specification (EBTS) Version 10 or later (for latent / ten print printers, latent / ten print display stations and latent and ten print scanners). (M)

2. The AFIS/VSS/LCMC/Transcoder renewal solution scanners must support all the scanning related requirements stated throughout this SOW and its accompanying documents. (M)

3. Hand held cameras must support scanning a barcode as stated in the requirements throughout this SOW and its accompanying documents. (M)

3.3.3 PRINTERS

1. Printers provided with the AFIS/VSS/LCMC renewal solution shall meet, at a minimum, the Image Quality Specification (IQS) of Appendix F in the Electronic Biometric Transmission Specification (EBTS) Version 10 or later (for latent / ten print printers, latent / ten print display stations and latent and ten print scanners). (M)

2. Printers supplied with the AFIS/VSS/LCMC shall include a calibration feature. (M)

3. The AFIS/VSS/LCMC renewal solution printers must support all the printing related requirements stated throughout this SOW and its accompanying documents. (M)

3.3.4 SAN STORAGE

1. The amount of on-line storage space for the new solution is highly dependent upon the Contractor's physical implementation of the functional requirements. A table of today's storage requirements, together with the estimated increase in transaction volumes is provided to aid the Contractor in estimating the overall storage requirements for the AFIS renewal solution. The Contractor shall specify the on-line storage capacity required on the RCMP SAN for its AFIS renewal solution (Primary site, DR site and backup). (M)
2. The AFIS/VSS/LCMC renewal solution should provide efficient and effective use of SAN storage. (R)
3. The RCMP recognizes that on-line storage to accommodate temporary files will be required for the conversion of today's information prior to its incorporation in the AFIS renewal Solution. The Contractor shall specify the storage capacity required on the RCMP SAN for the conversion activities. This space shall be freed up upon completion of the conversion. (M)

3.3.5 CAMERAS

1. The GFE cameras are end-of-service and must be replaced. The replacement cameras must support the following requirements, in addition to the requirements stated throughout the SOW and its accompanying documents: (M)
    a. The fingerprint technician must be able to use a single action (e.g. mouse click on a button) to activate using the camera;
    b. For barcode scanning the fingerprint technician will:
        i. Place the paper fingerprint form under the camera,
        ii. The UI will display the portion of the paper that is viewable with the camera,
        iii. The camera will automatically read the barcode and populate a search field with the contents of the barcode (e.g. File number), and
        iv. The user will initiate a fetch using a single action (e.g. mouse click), which will fetch the prints and start the camera certify process (cold certify);
    c. For the camera certify process the fingerprint technician will:
        i. Move the paper form around to position the paper for viewing one of the images under the camera, and
        ii. The camera must be capable of displaying a full fingerprint for the user to use in a side-by-side comparison;
    d. The camera certify process shall enable a technician to adjust the image being viewed with the camera, to enable the analysis of the image, with at least the following capabilities using a variable sizing capability with a mouse controlled method such as, hover and scroll, or slider; to finely tune the adjustments. Additionally, there must be a reset button for each of these functions to remove the specific image adjustments:

   i. Zoom in / zoom out an image,

   ii. Adjust brightness, and

   iii. Adjust background brightness (contrast);

e. Provide a button or similar method to reset all of the image adjustments; and

f. Allow the most common settings for the image adjustments to be pre-set and used as the initial settings for an image display.

3.3.6 SOFTWARE

1. The RCMP has a comprehensive suite of software products for which it has negotiated licences and support agreements. (I)
2. However, RCMP understands that the AFIS/VSS/LCMC renewal solution may include additional software products for which licences and support agreements will be required. (R)
3. The Contractor will be responsible for providing licenses and support for all non-GFE software products. The Contractor will also be responsible for upgrades/changes to GFE software as indicated in Section 4.7 GFE Clarification and throughout this SOW and its accompanying documents. The Contractor's proposal must explain how each software product is used by the AFIS renewal solution to satisfy the requirements stated throughout this SOW and its accompanying documents. (M)
4. COTS software provided as part of the AFIS/VSS/LCMC renewal solution is expected to be specific to the solution. In other words, the Contractor is not expected to provide any standard Office Automation (OA) products (e.g. e-mail, word processing, and spreadsheet) as the RCMP currently have negotiated licences for its standard suite of OA products. (I)
5. Additionally, the RCMP has license to other software used as part of the current solution which has been identified throughout this SOW and its accompanying documents. (I)

4. OVERVIEW OF RENEWAL APPROACH

4.1 Purpose

1. This section provides an overview of what environments are available and possible uses of the environments, with the Entire AFIS renewal solution, that can be supported by RCMP. This information is not intended to define or suggest a specific approach. (I)
2. This section also describes what is expected to be accomplished with the complete renewal and how the following sections of the document provide specific details concerning each key area of RTID to be renewed. (I)

4.2 Overall Approach

1. There are currently three (3) test environments DEVTEST, QCS and MAINT and the production environment, PROD. This AFIS renewal must replace, upgrade or reuse every server/workstation/Transcoder in all environments that results in satisfying, all the requirements, in all environments according to this SOW and its accompanying documents. (M)
2. The RCMP will establish a separate RTID test environment for the AFIS renewal solution which will be referred to herein as the AFIS-Renew environment. This AFIS-Renew environment will be available for the Contractor to use in the same or similar manner that the MAINT environment is typically used. That is, the MAINT environment is typically the environment used by the Contractor, in the normal RTID release process, to test their initial site installation of any new hardware and/or upgraded OS, software or DB to allow integration testing with RTID to be performed prior to delivery to the RCMP. This AFIS-Renew environment will have dual AFIS electronic sync filing capability provided by the NNS. This allows the flexibility for the Contractor to use the normal RTID release process and/or the AFIS-Renew environment with electronic sync filing as required; and have multiple releases to satisfy all requirements as stated in this RFP. (I)
3. To ensure flexibility for the Contractor to use the GFE and allow the RCMP to be prepared for the AFIS renewal, the DEVTEST environment must remain as is until after final acceptance of implementation stage 1. The DEVTEST environment will be used to support existing production until the cut-over to the AFIS/Transcoder/VSS renewal solution has been completed. (M)
4. The Contractor’s approach must ensure that it can be verified, by the RCMP, that the AFIS renewal solution satisfies all aspects of all functional, technical, interface and processing requirements for a test environment including support for the interface specifications and ICDs. (M)
5. The Site Acceptance Test Plans (SATPs) and Site Acceptance Test Reports (SATRs) identify the minimum that must be provided by the Contractor to demonstrate that its AFIS renewal solution satisfies all the requirements stated in this SOW and its accompanying documents. (M)

6. Following verification by the Contractor that all aspects of the Entire AFIS renewal solution satisfies all RTID interface and processing requirements, the RCMP will start its site acceptance testing. This site acceptance testing by the RCMP will include testing all AFIS and RTID functionality by the RTID test team. (I)

7. After RCMP approval of the AFIS renewal solution in a test environment, the AFIS renewal solution could follow the RTID release process or the RCMP agreed to adjustment to the release process in the Contractor's AFIS Renewal Implementation Plan (ARIP) (DID AR-01). (R)

8. The Contractor can configure an initial production environment that partially supports the full production requirements, with capacity that supports at least 80% of the 2019 Latent forward search volumes and 50% of all other 2019 volumes, and then reuse existing production servers after the cut-over to achieve one hundred percent (100%) capacity. The ARIP should show how the GFE and any other Contractor provided components are used to achieve one hundred percent (100%) capacity. (R)

9. The Contractor's proposed ARIP and supporting documentation should ensure the most effective and efficient approach is used to implement and make operational the AFIS renewal solution. There should be a focus on minimizing the overall operational outage time, minimizing the risk to RCMP RTID/AFIS operations, limiting the number of extended outages (see below paragraph 10), ensuring High Availability (HA) capabilities can be verified before production release and satisfying all requirements stated throughout this RFP in a timely manner. The precise length of each outage required must be identified in the ARIP and SATP with justification for each step in the implementation plan. Any consideration that ensures the integrity of RTID operations should be presented by the Contractor (R)

10. The normal RTID release window is twelve (12) hours from Saturday night at 2300 hours until Sunday morning at 1100 hours. For unusual circumstances, a maximum forty-eight (48) hour extended outage can occur from Friday night at 1800 hours until Sunday night at 1800 hours. Outages must fit within these release windows. (M)

11. To ensure the above flexible use of environments is clear, the following provides point form descriptions of possible uses: (I)

    a. DEVTEST will be available for RCMP to support the existing AFIS;

    b. The other test environments and their GFE are available for the Contractor's use; however, there must be at least one test environment and at least one other environment where QCS testing can be performed for any release. That is, the QCS environment could be used for QCS testing or the parallel production environment can be used for QCS testing prior to its acceptance and release for production use meaning the pre-production AFIS renewal solution would first serve as a QCS testing environment and then once accepted become the production AFIS renewal solution. In this instance a site fail-over test will also be completed as part of the QCS testing on the pre-production AFIS renewal solution;

    c. Once the AFIS renewal solution has been accepted in production, the QCS environment must be made fully operational for QCS testing before any other release can be tested. That is, if the parallel production AFIS renewal solution approach is used for a release with QCS testing in the pre-production configuration, once it is accepted in production, all other releases must be tested in the QCS environment prior to release to production; since this would mean that the AFIS renewal solution is in production and it could no longer be used for testing; and

d. The parallel Production AFIS renewal solution must operate in the Production environment, at both PR and DR sites, in parallel with the existing AFIS. That is, if the parallel production AFIS renewal solution approach is used for a release, it must operate in the Production environment, at both PR and DR sites, in parallel with the existing AFIS. After verification by the RCMP that the parallel AFIS renewal solution fully supports all the requirements in this SOW and its accompanying documents, the existing AFIS would be disabled and the parallel AFIS/Transcoder/VSS renewal solution would become the system of record for AFIS processing.

12. If the GFE will be used to achieve one hundred percent (100%) capacity after an initial release, the AFIS Renewal solution Production environment must support, at a minimum, at least 80% of the 2019 Latent forward search volumes and 50% of all other 2019 volumes with the initial AFIS Renewal production environment solution to ensure existing RCMP RTID production capacity can be supported until the GFE is used to achieve one hundred percent (100%) capacity. That is, the initial AFIS Renewal solution production environment acceptable to the RCMP must at least support 80% of the 2019 Latent forward search volumes and 50% of all other 2019 volumes before it can be considered for replacement of the existing AFIS solution; and then followed by an upgrade to hundred percent (100%) capacity using the GFE. (M)

13. The final ARIP is the deliverable that establishes the foundation for the execution of all aspects of this SOW. This deliverable must be completed and approved by the RCMP before work can start on any of the key areas to ensure the most cost effective and efficient implementation strategy can be developed and agreed to by the RCMP. This deliverable establishes the approach, and an overall strategy and plan that explains how each key area will be implemented. This deliverable is the Contractor’s opportunity to identify how the Contractor’s Entire AFIS renewal solution will be implemented within the RCMP/SSC security architecture. (M)

14. The SATP is based on the strategy and plan defined in the ARIP. The SATP provides the detailed installation activities, implementation steps and testing that must be completed in each site/environment that ensures the replacements/upgrades/reuse are effectively implemented according to the ARIP strategy and plan. (M)

15. As part of the normal release process, all applicable implementation steps developed by the Contractor in the SATP will be used by the RCMP to include in the RTID Release Implementation Plan for each site/environment. (M)

16. Server OSs that are, or will be, end-of-service before February 2020 must be upgraded or replaced by the Contractor at the Contractor’s cost. (M)

17. Server hardware that is end-of-life prior to 2010, even though its end-of-service is not declared, should not be used in the AFIS/VSS/LCMC renewal solution. (R)

4.3 Key Areas of Change

1. The relationship between each key area must be considered by the Contractor. Any dependencies between each key area must be identified to formulate an ARIP that allows all the work required in this SOW to be completed in the most effective and efficient manner that minimizes the impact to RTID test and Production environments. (M)
2. The Contractor must provide clear justification for the sequence of activities that minimizes any disruption to RTID test and/or Production environment operations. All the activities and scheduling details resulting from the ARIP must be provided to the RCMP for inclusion in the MCS. (M)
3. The Test environment replacement/upgrade/reuse changes must be included in the ARIP to ensure the RCMP release process can be followed for all releases following the cut-over to the AFIS/Transcoder/VSS renewal solution. (M)
4. The Transcoder upgrades must be fully tested and approved in the test environment before the Production Transcoders can be upgraded. Additionally, the Production Transcoder upgrade must be coordinated with agencies using the Transcoders to ensure minimal impact to remote agency operations and the RNSC. (M)
5. Workstation upgrades must be fully tested and approved before Production workstations can be upgraded. Five (5) existing PCS workstations will be allocated for the AFIS-Renew environment and Ten (10) existing PCS workstations will be allocated for the parallel AFIS renewal production environment. (M)
6. Except for the Contractor's parallel production environment configuration being used for HA/QCS testing instead of the QCS environment; the QCS environment must be used to test all the HA capabilities of the Contractor's AFIS renewal solution, unless specifically stated herein (i.e. site fail-over). The RCMP will lead all testing in the QCS environment or in the parallel production environment being used for QCS testing for the AFIS renewal solution. (M)
7. The Contractor must configure and implement the QCS environment to support all the HA and QCS requirements stated throughout this SOW and its accompanying documents. Additionally, every possible Production scenario must be testable in the QCS environment and every Production component must be in the QCS environment. (M)
8. Any HA capabilities that can only be tested in the Production environment must be clearly identified in the Contractor's proposal and must be pre-approved by the RCMP in writing to be acceptable HA testing nuances or the proposal may be considered non-compliant. Site fail-over from the PR to DR is the only testing nuance not required in the QCS environment. Refer to subsection 3.3.3 in Annex A – Current Architecture for an example of HA testing in Production only. (M)

4.4 RCMP Acceptance

1. RCMP acceptance testing will only start after the Contractor has successfully demonstrated that the replaced/upgraded/reused components are fully operational.

The SATR must be completed to document the successfully demonstrated component(s) operation. (M)

2. Each key area of this SOW can be accepted separately or together with one or more other key areas depending on the strategy and plan developed in the ARIP; however, the production AFIS/Transcoder/VSS renewal solution must support all existing key areas before parallel operations can be started. (M)

3. RCMP acceptance will be completed in stages. Following the RTID release process or the RCMP agreed to ARIP release process, system testing and then QCS testing, with final acceptance in the Production environment. (I)

4. The primary method of acceptance will be testing of all RTID/AFIS functionality to ensure the Contractor’s AFIS renewal solution satisfies all requirements stated in this SOW and its accompanying documents. Additionally, all HA capabilities will be tested in the QCS environment. This SOW and its accompanying documents identify the minimum HA testing that must be testable in the QCS environment. (M)

5. If the parallel production AFIS renewal solution approach is used for a release with QCS testing in the pre-production configuration, then production site fail-over testing must be completed as part of the QCS testing on the pre-production AFIS renewal solution. (M)

6. All intrasite HA capabilities must be testable in the QCS environment. (M)

7. The QCS environment does not need to support site fail-over testing. (I)

8. The full scope of the existing testing that is used by the RCMP is available for the Contractor’s review as required. (I)

4.5 Implementation Stages

1. There will be two (2) distinct stages for implementing the requirements that must be included with the initial procurement associated with this AFIS Renewal RFP. The two (2) stages are: (M)

   a. Renewal of all AFIS related subsystems including AFIS, Transcoder and VSS. This also includes all installation, implementation, integration, conversion, interoperability and set-to-work activities required for the entire scope of work identified in this SOW that is applicable to these key areas. This first stage must provide a fully operational AFIS, Transcoder and VSS renewal solution fully supporting the requirements stated throughout this SOW and its accompanying documents; and

   b. Replacement of ELMO with LCMC which also includes all installation, implementation, integration, conversion, interoperability and set-to-work activities required for the entire scope of work identified in this SOW that is applicable to this key area as well as any other requirements not specifically associated with one of the key areas as stated in this SOW and its accompanying documents. This second stage must provide a fully operational LCMC solution fully supporting the requirements stated throughout this SOW and its accompanying documents.

   c. Note: ELMO cannot be replaced until after the AFIS, Transcoder and VSS have been renewed and accepted in production by the RCMP.

2. To ensure it is clear, these two (2) stages must include installation, implementation, integration, conversion, interoperability and set-to-work activities required for all environments, following the RCMP / Chief Information Officer (CIO) release process or the RCMP agreed to process in the ARIP. (M)

3. All the training required with this initial procurement will be completed in stage one (1) or stage two (2). (M)

4. It is preferred that the implementation to support US EBTS Extended Feature Set (EFS) is completed as soon as possible. (R)

5. However, EFS must be implemented within two (2) years following contract award. This implementation of EFS must ensure backward compatibility to all existing data at the time of implementation, or conversion to EFS in a manner acceptable to the RCMP. As part of the EFS implementation, the Contractor must define a strategy to have EFS supersede the existing use of IAFIS Type-9 and ANSI INCITS 378-2004. (M)

6. This strategy should be included with the Contractor’s proposal which will be considered part of the evaluation assessing support for EFS. (R)

7. Facial recognition might be implemented at a to be determined date; however, the Contractor must support facial recognition capabilities to ensure RCMP will be able to support this additional biometric capability through a single vendor. (M)

4.6 Sync Filing During Parallel AFIS Operation

1. Throughout this SOW and its accompanying documents there are specific requirements stated regarding sync filing during parallel AFIS operation. The following provides a summary of the sync filing requirements that must be satisfied during parallel operations: (M)

   a. The AFIS Renewal solution must process packets received from NNS and record responses normally sent to NNS in a log file accessible by the RCMP. The NIST packets will be as defined in the AFIS ICD; therefore, the Contractor solution is expected to fully process the packet based on the content of the NIST packet in the normal production manner (i.e. except for the responses to NNS).

   b. The RCMP fingerprint and business staff will process any transactions requiring manual intervention on the AFIS Renewal solution.

   c. Latent sync filing transactions will not be submitted through NNS. Latent minutia, plotted by RCMP, must be retained for Latent data. To maintain synchronization with the existing AFIS, the AFIS Renewal solution must process the Latent additions and deletions.

   d. These additions and deletions will be provided by the RCMP weekly for processing in a NIST packet formatted like the data conversion Latent NIST packets. Since the risk of potential misses on the AFIS Renewal during parallel operation due to the Unsolved Latent File (ULF) being one week behind is low, the Latent volumes are low and NNS cannot effectively deliver RCMP plotted minutia in an automated manner; this is considered the most effective method. It is expected that the Contractor will reuse the Latent data conversion capability to support this requirement.

e. The Contractor must also provide a System Sync Filing Comparison report that is executed weekly to identify differences between the current AFIS and the AFIS Renewal solution. The RCMP will provide a report from the current AFIS identifying the following, which must be compared against the AFIS Renewal solution:

   i. Subject Id,

   ii. File number,

   iii. DCN, and/or

   iv. Latent image Id;

f. The Contractor's System Sync Filing Comparison report must provide any differences between the current AFIS and the AFIS Renewal solution in a format that can be used by a Microsoft Excel spreadsheet and easily identify which AFIS has, or does not have, which data. This report is expected to be run after the weekly Latent synchronization process. The Contractor's onsite staff and the RCMP will work together to resolve any differences that require a change on the AFIS Renewal solution; and

g. Note: Automated sync filing for Ten Print transactions is critical for RCMP to be able to automatically maintain the AFIS renewal solution TPF during parallel AFIS operation. It also allows the RCMP to verify that the AFIS and VSS renewal solutions are operating correctly and as expected against production data. The Ten Print volumes are very high which make the automated sync filing critical. Latents are low volume and can be reprocessed on the AFIS Renewal solution, as required, to verify that the Latent capabilities of the AFIS renewal solution are operating correctly and as expected against production data.

4.7 GFE Clarifications

1. The following clarifies the separation of responsibilities between the RCMP and the Contractor regarding the GFE. The specific requirements are stated throughout the SOW and its accompanying documents: (I)

   a. GFE Transcoder/AFIS workstations:

      i. The GFE Transcoder/AFIS workstations are currently configured with Windows 7. The license cost to upgrade these workstations, if required, to Windows 10 would be provided by the RCMP; and

      ii. All other changes required (e.g. changes to successfully pass a VA, configure for Contractor components, etc.) to support the Contractor's solution and satisfy the requirements stated in the SOW and its accompanying documents must be provided by the Contractor;

b. GFE servers:

   i. All GFE server changes, including operating system upgrades, must be provided by the Contractor,

   ii. The hardware maintenance contract for the GFE servers, as they are configured at the time of contract award, will be provided by the RCMP (i.e. GFE changes that increase the maintenance cost will be the responsibility of the Contractor), and

   iii. Since all OSs must be kept up-to-date, the latest service pack for any OS that will continue to be used must be included in the Contractor's implementation;

c. GFE Printers, Scanners and Cameras:

   i. All changes to the GFE printers and/or scanners required to support the Contractor's solution and satisfy the requirements stated in the SOW and its accompanying documents must be provided by the Contractor, and

   ii. GFE cameras are end-of-service and must be replaced. This includes a minimum of 25 cameras in the Production environment and 5 in the test environments. Refer to Appendix F for totals in each environment;

d. GFE load balancing and network connectivity:

   i. The RCMP will provide layer three (3) network components (layer three (3) switches with routing capabilities or equivalent layer three (3) router and layer two (2) switches) that can be used by Contractor's solution to support load balancing and network connectivity, and

   ii. The Contractor must ensure their solution works effectively with the RCMP load balancing to support all the requirements stated in this SOW and its accompanying documents;

e. GFE SAN:

   i. All SAN connectivity, including connectors and cabling to physically connect the servers to the RCMP will be provided by the RCMP according to the specifications identified in this SOW and its accompanying documents,

   ii. All server software, fiber channel network cards, firmware, etc. required to utilize the SAN connection must be provided by the Contractor,

   iii. All SAN storage required for Contractor's solution will be provided by the RCMP, and

   iv. The Contractor solution's use/consumption of SAN will be evaluated and must be provided with the proposal as part of the ARIP;

f. Simple Network Management Protocol (SNMP) reporting:

   i. The RCMP will provide an SNMP reporting system,

   ii. The Contractor must provide an SNMP Version 3 agent for each server that is part of their solution, and

iii. The RCMP can provide an SNMP agent for GFE servers that continue to use the same OS, if necessary;

g. Backup, Restore, Recovery:

i. The RCMP will provide the backup, restore, recovery products as stated in this SOW and its accompanying documents, and

ii. Anything other than what will be provided by the RCMP necessary to satisfy the requirements in this SOW and its accompanying documents, must be provided by the Contractor;

h. GFE WSUS and Anti-virus (ePo):

i. The RCMP environment supports providing WSUS updates to AFIS/Transcoder workstations and Windows servers,

ii. The RCMP environment supports providing McAfee anti-virus updates including client software on any supported device, and

iii. The operating system update and anti-virus update requirements that the Contractor must support are identified in this SOW and its accompanying documents;

i. Crystal Report:

i. The RCMP will provide the licenses for the users to use Crystal Reports Version 2013, and

ii. Any different version or different reporting software required by the Contractor's solution to satisfy the requirements stated in the SOW and its accompanying documents must be provided by the Contractor;

j. PC Duo:

i. The RCMP will provide the licenses for PC Duo for use with the Transcoders for RNSC and Contractor onsite support staff as described throughout the SOW and its accompanying documents. The current version in use is 12.1.2035; and

k. Oracle:

i. The RCMP will provide the licenses for Oracle 10g, 11g and XE 11g (server and client).

5. CONTRACTOR CORPORATE AND MANAGEMENT REQUIREMENTS

5.1 Purpose

1. This section describes the corporate and management requirements to be satisfied by the Contractor. (I)

5.2 Planning and Oversight

5.2.1 GENERAL

1. The Contractor shall identify key team members that will be accountable for responding to requests and managing the Contract. The Contractor must provide resumes that describe the relevant qualifications and experience of each individual. (M)

5.3 Contractor Organization

5.3.1 CONTRACTOR ORGANIZATIONAL STRUCTURE

1. The Contractor must provide an organizational chart and associated text that describes the organization it proposes to address the requirements of this Contract. This description should address at least the following: (M)

   a. The proposed resources and their qualifications;

      i. The roles and responsibilities of each resource;

   b. The reporting relationship, including the resources reporting relationship to their senior management; and

      i. The interface points between the Contractor’s resources and RCMP resources that should include an executive sponsor and a Single-Point-Of-Contact.

5.3.2 EXECUTIVE SPONSOR

1. The Contractor should identify an executive sponsor with overall responsibility for meeting the terms and conditions of this Contract. The executive sponsor should have ultimate resolution and approval authority, for the Contractor, concerning the Contract resulting from this SOW. The executive sponsor is expected to directly resolve any issues relating to this Contract on behalf of the Contractor. The organizational structure should depict the ultimate authority of the executive sponsor. If the executive sponsor is not the ultimate authority, then the executive level that represents the ultimate authority must be identified as well as the types of decisions that are expected to be directed to the ultimate authority. (R)

5.3.3 SINGLE POINT OF CONTACT (SPOC)

1. The Contractor must identify a SPOC that will be assigned to the Contract resulting from this SOW that has the authority and responsibility to directly or indirectly action Task Authorizations TAs and reporting request, and perform the tasks associated with SOW and its accompanying documents. (M)
2. The Contractor's SPOC and any other proposed resources directly interacting with the RCMP must have good oral and written communication skills. (M)

5.3.4 TECHNOLOGY AND PROCESS

1. The Contractor should describe any tools and processes that they will use to perform the tasks required for this Contract. (M)

6. AFIS PRODUCTION AND THREE TEST ENVIRONMENT RENEWAL

6.1 Purpose

1. This section describes the high-level functional and technical requirements for replacing/upgrading/reusing all AFIS Production and test environment components. These components must be replaced, upgraded or reused in a manner that fully supports all Production environment requirements as stated in this SOW and its accompanying documents. The detailed requirements that must be satisfied by the Contractor's AFIS renewal solution are described in Annex B. (M)

6.2 GFE Components

1. Annex F provides a list of all GFE available for use by the Contractor. The Contractor's proposal must explain how each GFE component will be modified and/or used together with all other Contractor components to provide the AFIS renewal solution. The Contractor must include the use of these components in the ARIP and SATP. (M)
2. The Contractor must ensure that the modifications are completed in the most effective and efficient method; and must ensure the modifications can be completed within the normal outage time for Production RTID. The RCMP must approve the method and timing of any modifications to GFE components. (M)

6.3 Common Environment Requirements

6.3.1 GENERAL

1. This section describes the common high-level functional and technical requirements that the Contractor must support for all the Production and test environments. Refer to Annex A for a more detailed description of how these AFIS environments are currently used. These current AFIS architecture requirements that must be supported are vendor independent capabilities that ensure the RCMP RTID test environments can operate in an effective and efficient manner as well as enable all Production AFIS functional and technical requirements to be effectively tested. (M)

6.3.2 FUNCTIONALITY

1. The Production environment must support all requirements as stated in this SOW and its accompanying documents. All test environments must provide all the functionality available in the Production environment, unless otherwise specifically stated in this SOW. (M)

6.3.3 LOAD BALANCING SCALABILITY WITH CISCO LB/SSL

1. For security, performance, scalability and load balancing reasons, the RCMP has implemented Open Systems Interconnection (OSI) layers 4–7 content switching with load balancing and Network Address Translation (NAT) support through Cisco

network devices configured with LB/SSL modules. This load balancing enables application and/or service requests to be directed to a virtual server and then distributed to multiple servers managed by the load balancing. NAT allows the Internet Protocol (IP) addresses of the real servers to be concealed and transparent to the requester. NAT translates the IP address used in the request to the IP addresses of the real servers. This combination of services allows requests to be sent to a Virtual IP address (VIP), to conceal the real IP address and greatly improve performance by creating a scalable environment. This capability is also used to direct requests, based on content to the appropriate server. Additionally this network level load balancing inherently provides intra-site and inter-site fail-over at the network level. These are critical requirements that must be supported by the Contractor's AFIS renewal solution proposed to satisfy the requirements in this SOW. (M)

2. The Contractor's AFIS renewal solution must support the ability to use the RCMP's LB/SSL technology to enable load balancing to multiple Contractor servers providing intra-site and inter-site HA. (M)

3. The AFIS servers must be able to send responses to VIPs defined on the LB/SSL destined to RCMP servers. (M)

4. The Contractor's AFIS renewal solution must also support inter-site fail-over at the network level that allows AFIS DR operations to continue in case of a PR site failure. (M)

5. These load balancing and HA capabilities must be implemented in the PROD and QCS environments. The QCS environment must be able to support all possible Production scenarios, except inter-site fail-over, unless agreed to in writing by the RCMP. (M)

6. The specific load balancing techniques required by the Contractor's AFIS renewal solution must be explained in the Contractor's proposal. (M)

7. Any details concerning the RCMP LB/SSL can be provided by the RCMP upon request; however, LB/SSL related information is available online. (I)

8. All servers in the Entire AFIS renewal solution must support the Network Time Protocol (NTP) to maintain clock synchronization through the RCMP/SSC network devices. (M)

6.3.4 BACKUP, RESTORE AND RECOVERY

1. The Contractor's Production AFIS renewal solution and all test environments must support backup, restore and recovery using the RCMP Tivoli backup/restore/recovery facilities. Each environment must be configured to backup on a regularly scheduled basis as per RCMP guidelines. (M)

6.3.5 SAN CONNECTIVITY

1. Annex A describes the current AFIS architecture which includes SAN connectivity for the PROD and QCS environments. The Contractor's QCS AFIS renewal solution must support SAN connectivity that is configured in the same or similar manner as Production to ensure the QCS environment can be used to test all possible Production

scenarios. Additionally, the Contractor's PROD and QCS solution must use SAN backup, restore and recovery capabilities using RCMP's Hitachi Data Systems (HDS) Virtual Storage Platform (HVSP) SAN technology with true copy. As with any other AFIS environment, the PROD and QCS environments must also use RCMP Tivoli backup/restore/recovery facilities for non-SAN data. (M)

6.3.6 HIGH AVAILABILITY

1. The QCS environment must be configured with sufficient components in the same manner as the Production environment that allows all possible Production HA capabilities to be tested in the QCS environment, except inter-site fail-over. Refer to Annex A for a more detailed description of the requirements each AFIS environment must be able to support. (M)

6.3.7 SNMP REPORTING

1. The Contractor's servers in all environments must support SNMP reporting to RCMP's Spectrum/eHealth (or replacement) system monitoring solution. Any servers that cannot support RCMP's SNMP reporting must be pre-approved, in writing by the RCMP, prior to submitting the response to this SOW or the proposal may be considered non-compliant. (M)
2. This SNMP reporting must include automated system level monitoring capabilities, at the hardware and software application level, capable of producing SNMP traps/alerts when software or hardware faults are detected. The minimum SNMP reporting must include memory utilization, CPU utilization, disk utilization, key process failures and hardware faults. (M)

6.3.8 MCAFEE ANTI VIRUS (AV) SCANNING

1. The Contractor's servers in all environments must include McAfee AV scanning. (M)
2. Preferably the Contractor's servers should participate in RCMP's ePo. (R)
3. However, as a minimum the Contractor must have a regularly scheduled McAfee DAT file update process completed by the Contractor in a manner approved by the RCMP with a configuration management documented history of the updates. (M)
4. All Contractor AFIS workstations in all environments must participate in RCMP's ePo to automatically receive DAT file and policy updates. These updates will be automatically completed within an RCMP determined timeframe. The Contractor's solution must be able to support the automatic RCMP ePo updates. (M)
5. There are separate ePo containers for Production and test environments. There is flexibility to allow any AFIS workstations to be included in an ePo container. This allows testing of new policies for specific AFIS workstations to eliminate the potential impact of the new policies affecting AFIS workstation operations. The policies defined in these containers for AFIS workstations must be determined through the normal release process, testing AFIS in each test environment, prior to release in the Production environment. (M)

6.3.9 WINDOWS SERVER UPDATE SERVICES (WSUS)

1. All Contractor Windows servers, in all environments, must include Windows OS updates on a regular basis and must participate in RCMP's WSUS. Server updates are not automatically enforced to minimize the potential impact on Production operations; however, the Contractor must ensure the Windows servers are updated within the time frame defined by the RCMP. This time frame is typically within three (3) weeks of receiving the update; however, this timing can change based on RCMP policy decisions. (M)
2. All the Contractor AFIS workstations, in all environments, must include Windows OS updates on a regular basis and must participate in RCMP's WSUS. Windows workstation updates are automatically enforced, typically within five (5) days. The Contractor's AFIS workstation solution must support receiving and automatically processing WSUS updates. (M)

6.3.10 ADDITIONAL OS AND SOFTWARE UPGRADES

1. Besides the WSUS automated OS updates, all other OS and software upgrades must be completed according to DID OU-01, Ongoing Updates. (M)

6.3.11 Environment CONSISTENCY

1. All test environments must be consistently configured, except for software differences that are expected through the normal release process and configuration parameters unique to an environment. That is, the Contractor must ensure the OS, software, AV DAT file and policies; and all other aspects of each component in each environment is consistent based on the function provided by the component. For example, all the Contractor test environment Web servers must use the same OS and third-party software versions that are also consistent with Production, unless the OS or third-party software is in the process of an upgrade. (M)
2. The QCS and PROD environments have HA capabilities which require a different configuration than the DEVTEST and MAINT test environments; however, the Contractor must still use the same common software and configuration parameters throughout the other test environments. For example, Contractor software that supports Web services in QCS and Production, where HA capabilities are required, must be the same software used in other test environments. (M)
3. The RCMP LB/SSL can load balance to multiple Web servers to provide HA; or to a single Web server to maintain a consistent configuration. To ensure environment consistency, test environments without HA capabilities must be configured in the same manner as the QCS/Prod environments with LB/SSL load balancing to a single server. (M)
4. Any inability to maintain this consistency among all environments must be specifically identified and agreed to in writing by the RCMP prior to the Contractor's proposal submission or the proposal may be considered non-compliant. (M)

6.3.12 SECURE SHELL (SSH) SPECIAL PORT

1. The Contractor must configure all test environments to use an RCMP designated port for SSH. The default port for SSH must not be used. This designated port will be provided by the RCMP after contract award. (M)

6.4 Common Test Environment Requirements

6.4.1 GENERAL

1. This section describes the high-level functional and technical requirements to be supported by the Contractor for all test environments. (I)
2. The replaced, upgraded or reused components must be implemented in a manner that ensures the test environments can be configured in the same, or similar, manner to the Production environment; and fully support all AFIS renewal functional and technical requirements. Other than configuration differences for communicating in different environments and reduced performance, there must be no differences between the Production and test environment AFIS renewal components unless agreed to in writing by the RCMP. (M)
3. Refer to Annex A for a more detailed description of how the environment capabilities in each AFIS test environment are currently used. These current AFIS architecture capabilities that must be supported are vendor independent features that ensure the RCMP RTID test environments can operate in an effective and efficient manner as well as enable all Production AFIS functional and technical requirements to be effectively tested. (M)

6.4.2 SUPPORT FOR MULTIPLE NNS ENVIRONMENTS

1. The AFIS DEVTEST environment must support multiple NNS Integration environments, multiple NNS Systest environments, multiple NNS performance environments and multiple individual developer environments. The AFIS DEVTEST must be configured initially to support at least 20 different NNS environments. Refer to Annex A for a more detailed description of the requirements each AFIS environment must support. (M)
2. The AFIS MAINT environment must support multiple NNS environments and multiple individual developer environments. The AFIS MAINT must be configured initially to support at least five (5) different NNS environments. (M)

6.4.3 TEST ENVIRONMENT PERFROMANCE REQUIREMENTS

1. The current DEVTEST environment database size is: (I)
   a. 5000 Ten Print records;
   b. 1534 Finger Latents;
   c. 204 Palm Latents; and
   d. All test environments are similar in size.

2. Based on a growth of five percent (5%) per year, each test environment must meet or exceed the following performance measurement requirements for the next five (5) years: (M)

   a. Process 220 transactions per hour, based on 200 Ten Print and 20 finger/palm latent transactions per hour from one NNS environment without negatively affecting any other NNS environment using the DEVTEST AFIS; and

   b. Where the performance measurement is based on the time AFIS requires to fully process the transaction and respond to RCMP NNS Web service interface.

6.5 Specific Test Environment Requirements

6.5.1 AFIS DEVTEST AND MAINT

6.5.1.1 General

1. The DEVTEST and Maint environments must be configured to support all the functional requirements of the AFIS Renewal solution. (M)

2. To ensure clarity regarding the functional requirements, if high performance hardware fingerprint matching components are part of the Contractor’s Production solution and the Contractor has low performing matching components that fully support the fingerprint matching and functional requirements as well as the common test environment requirements, then the low performing matching components can be used instead of high performance hardware fingerprint matching components in these two (2) test environments. (I)

6.5.2 AFIS QCS

6.5.2.1 General

1. The QCS environment must be configured with every possible Production component in the Contractor’s AFIS renewal solution. These components must be configured in a manner that allows every possible Production scenario to be tested in the QCS environment, except inter-site fail-over. (M)

6.5.2.2 High Availability

1. The QCS environment must be configured with sufficient components in the same manner as the Production environment that allows all possible Production HA capabilities to be tested in the QCS environment, except inter-site fail-over. Refer to Annex A for a more detailed description of the requirements each AFIS environment must be able to support. (M)

6.6 Production Environment Requirements

6.6.1 GENERAL

1. This section describes the high-level functional and technical requirements to be supported by the Contractor for the PROD environment. (I)
2. This section describes the functional and technical requirements for replacing/ upgrading/reusing all PROD environment components. These components must be replaced, upgraded or reused in a manner that fully supports all Production environment requirements as stated in this SOW and its accompanying documents. (M)

6.6.2 CAPACITY AND PERFORMANCE REQUIREMENTS

1. The Contractor must ensure all capacity and performance requirements stated in this SOW and its accompanying documents are satisfied. The Contractor shall be responsible for ensuring the capacity and performance requirements are met regardless of whether the Contractor chooses to replace, upgrade or reuse any GFE components. Refer to Annex B for details concerning the AFIS renewal solution capacity and performance requirements. (M)
2. To ensure effective and efficient use of the AFIS renewal solution, the components that provide approximately fifty percent (50%) of the AFIS capacity must reside at the DR site and be active in AFIS processing. (M)
3. If the PR site fails, the AFIS renewal solution must support at least fifty percent (50%) of the AFIS capacity and performance requirements at the DR site. (M)

6.6.3 HIGH AVAILABILITY

1. The Contractor’s AFIS renewal solution must support all PR site HA requirements stated in this SOW and its accompanying documents. (M)
2. The Contractor’s AFIS renewal solution must support all the DR requirements stated in this SOW and its accompanying documents. The PROD environment is the only environment with DR site requirements. (M)
3. All Contractor DR site components must be configured in the same, or similar, manner to the PR site to ensure AFIS operations continue if there is a PR site failure. (M)

6.7 Site Acceptance Test Plan

1. The Contractor must provide a Site Acceptance Test Plan (SATP) DID AT-03 that describes all the activities necessary to replace, upgrade, reuse, configure and implement all components required to satisfy all AFIS renewal solution requirements. (M)

7. TRANSCODER RENEWAL

7.1 Purpose

1. This section describes the high-level functional and technical requirements for replacing/ upgrading/reusing all Transcoder Production and test environment components. These components must be replaced, upgraded or reused in a manner that fully supports all Production and test environment requirements as stated in this SOW and its accompanying documents. The detailed requirements that must be satisfied by the Contractor's Transcoder renewal are described in Annex C. (M)

7.2 GFE Components

1. The list of all GFE available for use by the Contractor, listed in Annex F, includes Transcoder components. The Contractor's proposal must explain how each GFE component will be modified and/or used together with all other Contractor components to provide the Transcoder renewal solution. The Contractor must include the use of these components in the ARIP and SATP. (M)
2. The Contractor must ensure that the modifications are completed in the most effective and efficient method; and must ensure the modifications can be completed within the normal outage time for Production RTID. The RCMP must approve the method and timing of any modifications to GFE components. (M)

7.3 Transcoder Common Requirements

7.3.1 GENERAL

1. The Transcoders must be replaced, upgraded or reused in a manner that ensures the Production and test environments are configured and maintained in the same manner and fully supports all Transcoder functional and technical requirements. Other than configuration differences for communicating in different environments, there must be no differences between the Production and test environment Transcoders unless agreed to in writing by the RCMP. (M)

7.3.2 FUNCTIONALITY

1. The Transcoder must support all requirements as stated in this SOW and its accompanying documents. The Transcoder is an input device to the NNS; therefore, all Transcoders in all environments must provide the same functionality. (M)

7.3.3 MCAFEE ANTI VIRUS (AV) SCANNING

1. All Contractor Transcoders in all environments must participate in RCMP's ePo to automatically receive DAT file and policy updates. These updates will be automatically completed with an RCMP determined timeframe. The Contractor's solution must be able to support the automatic RCMP ePo updates. (M)

2. There are separate ePo containers for Production and test environments. There is flexibility to allow any Transcoder to be included in an ePo container. This allows testing of new policies for specific Transcoders to eliminate the potential impact of the new policies affecting Transcoder operations. The policies defined in these containers for Transcoders must be determined through the normal release process testing Transcoders in each test environment prior to release in the Production environment. (M)

7.3.4 WINDOWS SERVER UPDATE SERVICES (WSUS)

1. All the Contractor Transcoders, in all environments, must include Windows OS updates on a regular basis and must participate in RCMP's WSUS. Windows workstation updates are automatically enforced. The Contractor's Transcoder solution must support receiving and automatically processing WSUS updates. (M)

7.4 Site Acceptance Test Plan

1. The Contractor must provide a Site Acceptance Test Plan (SATP) DID AT-03 that describes all the activities necessary to replace, upgrade, reuse, configure and implement all components required to satisfy all Transcoder renewal solution requirements. (M)

8. VERIFICATION SUBSYSTEM AND THREE TEST ENVIRONMENT RENEWAL

8.1 Purpose

1. This section describes the high-level functional and technical requirements for replacing/ upgrading/reusing all VSS Production and test environment components. These components must be replaced, upgraded or reused in a manner that fully supports all Production environment requirements as stated in this SOW and its accompanying documents. The detailed requirements that must be satisfied by the Contractor's VSS renewal solution are described in Annex D. (M)

8.2 GFE Components

1. Annex F provides a list of all GFE available for use by the Contractor. The Contractor's proposal must explain how each GFE component will be modified and/or used together with all other Contractor components to provide the VSS renewal solution. The Contractor must include the use of these components in the ARIP and SATP. (M)
2. The Contractor must ensure that the modifications are completed in the most effective and efficient method; and must ensure the modifications can be completed within the normal outage time for Production RTID. The RCMP must approve the method and timing of any modifications to GFE components. (M)

8.3 Common Environment Requirements

8.3.1 GENERAL

1. This section describes the high-level functional and technical requirements that the Contractor must support for all VSS Production and test environments. Refer to Annex A for a more detailed description of how these requirements in each AFIS environment are currently used. These current VSS architecture requirements that must be supported are vendor independent capabilities that ensure the RCMP RTID test environments can operate in an effective and efficient manner as well as enable all Production VSS functional and technical requirements to be effectively tested. (M)
2. The replaced, upgraded or reused components must be implemented in a manner that ensures the test environments can be configured in the same, or similar, manner to the Production environment; and fully support all RTID VSS functional and technical requirements. Other than configuration differences for communicating in different environments and reduced performance, there must be no differences between the Production and test environment VSS renewal components unless agreed to in writing by the RCMP. (M)

8.3.2 FUNCTIONALITY

1. The Production environment must support all requirements as stated in this SOW and its accompanying documents. All test environments must provide all the functionality

available in the Production environment, unless otherwise specifically stated in this SOW. (M)

8.3.3 LOAD BALANCING SCALABILITY WITH CISCO LB/SSL

1. The Contractor’s VSS renewal solution must support the ability to use the RCMP’s Cisco LB/SSL technology to enable load balancing to multiple Contractor servers providing intra-site and inter-site HA. (M)
2. The Contractor’s VSS renewal solution must be configured to support a dual Data Center architecture that allows the DR site VSS components to continue working without interruption if the PR site fails. (M)
3. The load balancing and HA capabilities must be implemented in the PROD and QCS environments. The QCS environment must be able to support all possible Production scenarios unless agreed to in writing by the RCMP, except inter-site fail-over. (M)
4. The Contractor’s VSS solution must support load balancing techniques that evenly load balance to at least four (4) VSS nodes, with two (2) nodes at the PR site and two (2) nodes at the DR site. (M)
5. Any details concerning the RCMP LB/SSL can be provided by the RCMP upon request. (I)

8.3.4 BACKUP, RESTORE AND RECOVERY

1. The Contractor’s Production VSS renewal solution and all test environments must support backup, restore and recovery using the RCMP Tivoli backup/restore/recovery facilities. Each environment must be configured to backup on a regularly scheduled basis as per RCMP guidelines. (M)

8.3.5 SAN CONNECTIVITY

1. Annex A describes the current AFIS architecture which includes SAN connectivity for the PROD and QCS environments. The Contractor’s QCS VSS renewal solution must support SAN connectivity that is configured in the same or similar manner as Production to ensure the QCS environment can be used to test all possible Production scenarios, except inter-site fail-over. (M)
2. Additionally, the Contractor’s PROD and QCS solution must use SAN backup, restore and recovery capabilities using RCMP’s HDS VSP SAN technology with true copy. As with any other VSS environment, the PROD and QCS environments must also use RCMP Tivoli backup/restore/recovery facilities for non-SAN data. (M)

8.3.6 HIGH AVAILABILITY

1. The VSS QCS environment must be configured with sufficient components in the same manner as the Production environment that allows all possible Production HA capabilities to be tested in the QCS environment, except inter-site fail-over. (M)

8.3.7 SNMP REPORTING

1. The Contractor's VSS servers in all environments must support SNMP reporting to RCMP's Spectrum/eHealth (or replacement) system monitoring solution. Any servers that cannot support RCMP's SNMP reporting must be pre-approved prior to submitting the response to this SOW in writing by the RCMP or the proposal may be considered non-compliant. (M)
2. This SNMP reporting must include automated system level monitoring capabilities, at the hardware and software application level, capable of producing SNMP traps/alerts when software or hardware faults are detected. The minimum SNMP reporting must include memory utilization, CPU utilization, disk utilization, key process failures and hardware faults. (M)

8.3.8 MCAFEE ANTI VIRUS (AV) SCANNING

1. The Contractor's servers in all environments must include McAfee AV scanning. (M)
2. Preferably participating in RCMP's ePo. (R)
3. However, as a minimum the Contractor must have a regularly scheduled McAfee DAT file update process completed by the Contractor in a manner approved by the RCMP with a configuration management documented history of the updates. (M)

8.3.9 WINDOWS SERVER UPDATE SERVICES (WSUS)

1. All Contractor Windows servers, in all environments, must include Windows OS updates on a regular basis and must participate in RCMP's WSUS. Server updates are not automatically enforced to minimize the potential impact on Production operation; however, the Contractor must ensure the Windows servers are updated within the time frame defined by the RCMP. This time frame is typically within three (3) weeks of receiving the update; however, this timing can change based on RCMP policy decisions. (M)

8.3.10 ADDITIONAL OS AND SOFTWARE UPGRADES

1. Besides the WSUS automated OS updates, all other OS and software upgrades must be completed according to DID OU-01, Ongoing Updates. (M)

8.3.11 ENVIRONMENT CONSISTENCY

1. All test environments must be consistently configured, except for software differences that are expected through the normal release process and configuration parameters unique to an environment. That is, the Contractor must ensure the OS, software, AV DAT file and policies; and all other aspects of each component in each environment is consistent based on the function provided by the component. For example, all the Contractor test environment Web servers must use the same OS and third-party software versions, that are also consistent with Production, unless the OS or third-party software is in the process of an upgrade. (M)

2. The VSS QCS and PROD environments have HA capabilities which require a different configuration than the DEVTEST and MAINT test environments; however, the Contractor must still use the same common software and configuration parameters throughout the other test environments. For example, Contractor software that supports Web services in QCS and Production, where HA capabilities are required, must be the same software used in other test environments. (M)

3. To ensure environment consistency, test environments without HA capabilities must be configured in the same manner as the QCS/Prod environments with LB/SSL load balancing to a single server. (M)

4. Any inability to maintain this consistency among all environments must be specifically identified and agreed to in writing by the RCMP prior to the Contractor's proposal submission or the proposal may be considered non-compliant. (M)

8.3.12 SSH SPECIAL PORT

1. The Contractor must configure all environments to use an RCMP designated port for SSH. The default port for SSH must not be used. This designated port will be provided by the RCMP after contract award. (M)

8.4 Common Test Environment Requirements

8.4.1 GENERAL

1. This section describes the high-level functional and technical requirements that the Contractor must support for all VSS test environments. (M)

2. The replaced, upgraded or reused components must be implemented in a manner that ensures the VSS test environments can be configured in the same, or similar, manner to the VSS Production environment, and fully support all RTID VSS functional and technical requirements. Reduced performance in the test environments is the only aspect of the Contractor's solution that can be different from the Production environment. (M)

3. Refer to Annex A for a more detailed description of how the environment capabilities in each VSS test environment are currently used. These current VSS architecture capabilities that must be supported are vendor independent features that ensure the RCMP RTID test environments can operate in an effective and efficient manner as well as enable all Production VSS functional and technical requirements to be effectively tested. (M)

8.5 Specific Test Environment Requirements

8.5.1 VSS QCS

8.5.1.1 General

1. The VSS QCS environment must be configured with every possible Production component in the Contractor's VSS renewal solution. These components must be

configured in a manner that allows every possible Production scenario to be tested in the QCS environment, except inter-site fail-over. (M)

8.5.1.2 High Availability

1. The VSS QCS environment must be configured with sufficient components in the same manner as the Production environment that allows all possible Production HA capabilities to be tested in the QCS environment, except inter-site fail-over. (M)

8.6 Production Environment Requirements

8.6.1 GENERAL

1. This section describes the high-level functional and technical requirements to be supported by the Contractor for the PROD environment. (I)
2. This section describes the functional and technical requirements for replacing/upgrading/ reusing all PROD environment components. These components must be replaced, upgraded or reused in a manner that fully supports all Production environment requirements as stated in this SOW and its accompanying documents. (M)

8.6.2 CAPACITY AND PERFORMANCE REQUIREMENTS

1. The Contractor must ensure all capacity and performance requirements stated in this SOW and its accompanying documents are satisfied. The Contractor shall be responsible for ensuring the capacity and performance requirements are met regardless of whether the Contractor chooses to replace, upgrade or reuse any GFE components. (M)
2. To ensure effective and efficient use of the VSS renewal solution, the components that provide approximately fifty percent (50%) of the VSS capacity must reside at the DR site and be active in AFIS processing. The VSS is a dual Data Center architecture; therefore, all VSS components must be fully utilized at both the PR and DR sites. (M)
3. If the PR site fails, the VSS renewal solution must support at least fifty percent (50%) of the VSS capacity and performance requirements. (M)

8.6.3 HIGH AVAILABILITY

1. The Contractor’s VSS renewal solution must support all PR site HA requirements stated in this SOW and its accompanying documents. (M)
2. The Contractor’s VSS renewal solution must support all the DR requirements stated in this SOW and its accompanying documents. The PROD environment is the only environment with DR site requirements. (M)
3. All Contractor DR site components must be configured in the same manner to enable dual Data Center operations. (M)

8.7 Site Acceptance Test Plan

1. The Contractor must provide a Site Acceptance Test Plan (SATP) DID AT-03 that describes all the activities necessary to replace, upgrade, reuse, configure and implement all components required to satisfy all VSS renewal solution requirements. (M)

9. LATENT CASE MANAGEMENT CAPABILITY (LCMC)

9.1 Purpose

1. This section describes the high-level functional and technical requirements for the LCMC. The detailed requirements that must be satisfied by the Contractor's LCMC renewal solution are described in Annex E. (M)
2. The LCMC must be a replacement of the existing ELMO and must be an integrated solution with the Contractor's AFIS renewal solution. That is, the LCMC/AFIS users must be able to seamlessly interface between the LCMC and AFIS to send Latent fingerprints/palm prints for search from the LCMC and perform all other required capabilities stated in this SOW and its accompanying documents. (M)
3. The LCMC requirements must be satisfied using the same AFIS windows workstation to perform either LCMC or AFIS activities. Performing latent case management activities are part of the daily activities for an AFIS Latent Fingerprint Analyst. (M)
4. The preferred LCMC solution is an integrated capability within the AFIS. This would provide a consistent UI for the LCMC/AFIS users and ensure there is no duplication of capabilities or data in LCMC and AFIS. That is, this integrated LCMC capability would be part of the AFIS renewal solution UI, where additional buttons or UI icons on the AFIS renewal solution UI would be clicked by the user to perform case management activities. (R)
5. ELMO currently records in its database a significant portion of data that is also recorded in AFIS. The LCMC should eliminate all of this duplication. (R)
6. The LCMC must eliminate all this duplication from an AFIS/LCMC user perspective. That is, with an integrated LCMC solution, this duplication would be inherently eliminated. If the Contractor's chooses a third-party or separate LCMC, the Contractor must ensure any duplication between the LCMC and the AFIS renewal solution is seamless to the user. (M)
7. The Contractor's solution must include the database conversion from the existing ELMO SQL database to the Contractor's LCMC/AFIS database. (M)

10. TRAINING

10.1 Purpose

1. Most of the RCMP fingerprint technicians have many years of experience. The RCMP also has a comprehensive in-house training program with a classroom setup. The RCMP employs a train the trainer approach to any new systems. Consequently, the training required for the AFIS renewal RFP is ten (10) days of time from the Contractor’s senior trainer. If there are separate trainers for TP vs latent, then the RCMP will determine the portion of time to be used by each senior trainer after contract award. The Contractor must include ten (10) days of training by a senior trainer in its proposal to cover the training requirements for this AFIS renewal RFP. (M)

2. The ten (10) training days will be used during the first year of the contract. All travel costs by the trainer is subject to Government Of Canada travel expenses. These travel expense are billed separately from the Contractor’s bid and will be paid through a Task Authorization, if required, once a training schedule has been agreed to between the Contractor and the RCMP. (I)

3. Any additional training beyond the ten (10) days will be completed through a separate Task Authorization as required. (I)

11. ONGOING OS, SOFTWARE AND VIRUS UPGRADES

11.1 Purpose

1. This section describes the requirements for the Contractor to provide ongoing OS and software upgrades for all components included in the Contractor's AFIS renewal solution. (I)
2. Note: Transcoders procured directly by other Police agencies are not included in this SOW. They are expected to have a separate support contract. (I)

11.2 Background

1. The other sections throughout this SOW represent work to be completed by the Contractor to replace, upgrade or reuse all existing RTID AFIS solution components as well as add new capabilities such as LCMC. The ongoing OS and software work, identified in this section, is expected to start after the Contractor's initial solution has been fully implemented and all components included in this SOW have been replaced, upgraded or reused. (I)

11.3 Requirement

1. The following sub-sections identify general requirements for the ongoing OS and software upgrade; however, the detailed requirements of what must be provided and the deliverables required for this requirement are included in the DID OU-01. (M)
2. In general any OS and/or software upgrade completed by the Contractor must not negatively affect the functionality, security, availability, maintainability, scalability, manageability, configurability or the quality of the results experienced by the Entire AFIS renewal solution. Additionally, the improved capacity and performance achieved through the replacements/upgrades/reuse in this SOW must not be negatively affected by any OS and/or software upgrade completed by the Contractor, unless agreed to with the RCMP in writing. (M)
3. All the Contractor's Entire AFIS renewal solution servers must be upgraded based on the frequency and timing stated herein (Subsection 11.3.2), unless otherwise agreed to by the RCMP in writing. (M)

11.3.1 DSB VA

1. Any new service pack or new version of the OS and/or software included in an upgrade through the ongoing OS and Software Upgrade activity must successfully pass a DSB VA. (M)

11.3.2 UPGRADE FREQUENCY AND TIMING

1. Each set of the servers that provide the same function must be upgraded at the same time unless otherwise agreed to by the RCMP in writing. For example, it would be expected that all Web servers would be upgraded at the same time. However, all

servers could be updated at the same time if there is justification for this approach or the server upgrades can be staggered such that each set of servers providing the same function are updated on the same cycle to mitigate the risk of changing too many servers at the same time. The Contractor must provide the most effective and efficient upgrade method that allows all servers to be maintained in a manner that provides an acceptable level of risk as agreed to by the RCMP. (M)

2. Once all servers have been upgraded through replacement/upgrade/reuse or through this ongoing upgrade process, they must be continuously upgraded every three (3) months with at least the latest security patches that RCMP determines should be included. RCMP will provide a list of all security patches that they deem essential for any RCMP servers. (M)

3. All servers must be upgraded with any new OS service packs within one (1) year of their availability unless agreed to by the RCMP in writing. (M)

4. This ongoing OS and software upgrade must be provided following the completion of all other work in this SOW until the end of the contract and any option years that are exercised by the RCMP. The ongoing OS and software upgrade strategy and plan (DID OU-01) must be organized to allow costing to be provided on a yearly basis. The resources and activities in the strategy and plan must be provided at a level of detail that easily correlates to the Basis of Payment. (M)

11.3.3 AV SCANNING DAT FILES AND POLICIES

1. AV scanning DAT files and policy requirements are defined throughout this SOW. The Contractor must keep the AV DAT files and policies up-to-date on all servers as part of the on-going support process. The record of updates to the DAT files and/or policies must be recorded in DID UO-01 or an alternate Contractor method approved by the RCMP. (M)

12. FACIAL RECOGNITION CAPABILITY (FRC)

12.1 General

1. This section describes the functional and technical requirements for the Facial Recognition Capability (FRC) solution. (I)

2. The Contractor must support an FRC that can be integrated into the Contractor's proposed AFIS renewal solution. This integration must provide a seamless interface for the NNS-AFIS based on a modified AFIS ICD. That is, the RCMP considers a FRC as another biometric for the AFIS to process; therefore the same interface between NNS and AFIS would be used. To ensure it is clear to all Contractors, the only FRC mandatory requirement that must be satisfied, by the Contractor, at the time of proposal submission is a documented and demonstrated (i.e. at Benchmark testing) ability of the Contractor to support FRC. (M)

3. All other FRC requirements are provided to ensure the Contractor understands the current expectations of the RCMP regarding FRC. (I)

4. When implemented, the FRC must be fully operational as an integrated part of the AFIS renewal solution; therefore, all the operational requirements of the AFIS renewal solution must be extended to the FRC. For example, the availability, confidentiality, integrity, security, support, maintenance, bilingual UI and logging requirements for the AFIS renewal solution also apply to the FRC. (M)

12.2 FRC Requirements

1. The suspect photos will typically be from surveillance videos, Closed-Circuit Television (CCTV), hand held cameras including cell phones, or other non-controlled, poor-quality sources. In many cases, only partial facial images will be showing. The FRC is required to perform a one to one (1:1), and a one to many (1:N) digital facial comparisons. (I)

2. Prior to implementation, the FRC must support the following requirements: (M)

   a. Perform searches involving a known or unknown single photo to a target ID photo looking to confirm identity or suspected identity (1:1);

   b. Search the photo database using a known photo to discover if the person is in the AFIS/FRC database under other aliases (1:N);

   c. Search the photo database using an unknown photo to find a suspect and generate investigative leads (e.g. a surveillance camera photo from bank robbery matched against the photo database);

   d. Perform searches of the unknown photo database using a known photo (1:N) to find out if the current enrolled person was involved in previous crimes associated with that investigation;

   e. Perform searches of the unknown photo database using an unknown photo (1:N) to be used to generate investigative leads. (e.g. a surveillance camera photo matched against another surveillance camera photo from another crime scene establishing that the same person(s) are involved in both crimes);

f. Establish a composite (i.e. best set of photos) for all available photo pose angles for an individual that will be used for searching;

g. Be able to perform a batch search of the unknown photo database (many to many search), the results of which can be dispositioned by the biometric technician over an extended period of time. These will be done in instances where the photos of unknown persons are retrieved in bulk from a storage device;

h. Search tattoos and body marks;

i. Allow tattoos and body marks to be included in the AFIS renewal database for known individuals recorded in the AFIS database;

j. Use aging and weight loss/gain techniques to increase the probability of an ident; and

k. Use the ANSI NIST ITL1-2011 Type-10 specification.

3. Prior to implementation, the Contractor’s FRC shall provide tools to review captured photos, crop the quality face segments in the image, re-calibrate, enhance, edit, search and if there is no ident, store in the unknown photo database repository. The FRC shall be capable of saving the photos in an ANSI NIST ITL 1-2011 compatible format. (M)

4. The Contractor’s FRC should create photographic line-ups, with a configurable number of photos, based on specified parameters from a witness description. (I)

13. DATA CONVERSION

13.1 Purpose

1. This section describes additional requirements for the data conversion that have not been stated elsewhere in this SOW and its accompanying documents that must be satisfied by the Contractor. These additional requirements apply to all required data conversion unless specifically stated herein. (M)

2. For the Entire AFIS renewal solution, the Contractor must develop a comprehensive data migration plan for all data to be converted. An initial version of this Data Conversion Plan must be provided with the Contractor's proposal. The Data Conversion Plan must be included as part of the ARIP, where the Contractor must provide the strategy and plan for all activities required to satisfy the entire scope of requirements included in this SOW and its accompanying documents. (M)

3. The data conversion must be performed at RCMP's Ottawa, Ontario, Canada data center or an alternate RCMP/SSC data center, located in Ontario, Canada identified by the RCMP. The only potential variance will be the conversion of Transcoder data which can be controlled from Ottawa through a secure remote connection to the Transcoder site in order to complete the data conversion. (M)

4. The data conversion must include an audit trail of all conversion activity, which must include recording when any error occurs or when any data mapping occurs where the data is represented differently in the Contractor's solution than in the original data set. (M)

5. The existing RCMP AFIS database, IMM database, VSS database and Transcoder databases will be exported to ANSI NIST compliant formatted electronic files and include FBI EBTS Legacy IAFIS compliant Type-9 minutia records. The Contractor must complete the data conversion for AFIS, IMM, VSS and the Transcoders using the following data: (M)

    a. The TP / Palm Print (PP) NIST files are expected to include the following NIST records as applicable:

        i. Type-1 – Header,

        ii. Type-2 – Demographics,

        iii. Type- 4 Fingerprint Images,

        iv. Type-9 – Minutiae Record (FBI EBTS Compliant) (Contractor AFIS minutia is expected to be generated for TP data. If not, the Contractor must explain the impact of retaining the existing AFIS TP minutia on the Contractor's solution),

        v. Type-10 – Photo Image,

        vi. Type-14 – Fingerprint Images, and

        vii. Type-15 – Palm Print Images;

b. The TP/PP Type-2 record will provide all demographic information maintained on the AFIS database for the subject record;

c. The Latent (LT) / Palm Latent (PL) NIST files will include the following NIST records:

i. Type-1 – Header,

ii. Type-2 – Demographics,

iii. Type-9 – Minutiae Record (FBI EBTS Compliant) (Existing Latent minutia, plotted by RCMP, must be retained for LT data), and

iv. Type-13 – Latent Images;

d. The LT/PL Type-2 record will provide all demographic information maintained on the AFIS database for the latent case; and

e. The Contractor must ensure the NIST packets used in the conversion are retained representing the initial transaction used to populate the Contractor's solution.

6. The existing log files for AFIS, IMM, VSS and the Transcoders must be converted to a form searchable for historical and audit purposes and retained on the Contractor's solution where the data is accessible by RCMP resources and by remote site resources for Transcoder data. (M)

7. It is preferable that the converted log files could be used by the Contractor's solution. (R)

8. However, the log data must remain unaltered and searchable by the alphanumeric data to allow individual log records to be identified. (M)

9. The ELMO data that must be converted is described in detail in Annex E. (M)

10. The ELMO log files do not need to be converted, since the AFIS log files will be used to identify the historical activity against the case file data in ELMO. (I)

11. The AFIS and Transcoder user management database conversions must also adhere to the requirements herein and be described in the Data Conversion Plan. (M)

12. The Contractor shall produce a report; or reports for each type of conversion, of the findings at the conclusion of the loading of the data. (M)

13.2 Data Conversion Process

1. Data conversion refers to those activities and deliverables necessary to migrate existing AFIS data from the current AFIS to the AFIS renewal solution. (I)

2. No data conversion will be allowed until the RCMP has approved the final version of the Data Conversion plan. The Contractor's Data Conversion plan must be developed in collaboration with the RCMP to ensure all requirements and data nuances stated throughout this SOW and its accompanying documents are clearly understood and reflected in the Contractor's Data Conversion plan. (M)

3. The Contractor shall: (M)

    a. Identify changes in requirements that will affect data formats and develop a plan of action;

    b. Develop standard procedures for implementing conversions;

    c. Design, develop and implement conversion of legacy data formats to new formats; and

    d. Define quality standards for data conversion.

4. The RCMP will provide witnesses to the Data Conversion process to ensure completeness, accuracy and quality of all Conversion Operations. (I)

5. The Contractor shall prepare and document test cases, including expected results, for each conversion requirement. (M)

6. The Contractor shall carry out testing of the conversion software prior to Site Acceptance Testing. (M)

7. The Contractor, under the supervision of the RCMP, shall perform Site Acceptance Testing of data conversion software, utility(ies) and processes. (M)

8. The Contractor shall provide conversion statistics, including total number of records to be converted, total number successfully converted, problems encountered and their resolution. (M)

9. The Contractor shall provide controls to ensure that data converted maintains its integrity and referential integrity throughout all processing routines. (M)

13.3 Data Conversion Details

1. The Data Conversion process must maintain the data architecture of a single Subject filed to a single Subject Identifier, using the existing Subject Identifier. It is essential that the AFIS renewal solution retain the Subject Identifier relationship to an individual to support references to previously generated match reports and NNS audit log data. Inherently the relationship to all other file related data is also retained by using the existing AFIS Subject Identifier in the AFIS renewal solution database. (M)

2. The Contractor shall ensure that the single Subject Identification Number can include multiple sets of images and fingerprint characteristics. (M)

3. The Contractor shall ensure that the single Subject Identification Number includes up to six (6) file numbers, with four (4) currently implemented. Refer to the AFIS ICDs for details. (M)

4. The Contractor shall be responsible for loading all reference tables required for the AFIS solution. (M)

5. The Contractor shall be responsible for populating all administrator tables and configuration parameters. (M)

6. The Contractor shall provide the schema for all database tables to the RCMP, indicating which data fields shall be used for RCMP data and for what purpose. (M)

7. The Contractor shall carry out the Data Conversion process as per the approved Data Conversion Plan. (M)

8. The Contractor must account for and properly process the unique aspects of RCMP data identified in the ICDs and throughout this SOW and its accompanying documents (e.g. DCN format, DOC ID format, long and short forms of file numbers; and rules for consolidations of non A conversions as well as Refugee consolidations where 8500000 is smaller than 1000000). (M)

9. The data volumes are included in Annex B, AFIS detailed requirements. (I)

13.3.1 DATABASE CONVERSION NUANCES

1. The following two paragraphs identify nuances that must be used by the Contractor in the database conversion process, as well as in normal day-to-day processing when consolidations occur. (M)

2. For consolidations, involving two (2) or more Criminal records, the following ordinal numbering scheme must be used where appropriate to support the requirements stated through this SOW and its accompanying documents. (M)

    a. The short format of a Fingerprint Section (FPS) Number is either a 1 to 6 digit numeric or a 1 to 6 digit numeric + a letter. Forensic Identification Services (FIS) manages the allocation of FPS Numbers. When all the numbers are used up for a specific character, then the next alphabetic character to be used is selected. Each alpha character will last approximately six (6) years**.** The “G” series (i.e., 999999G) is currently being used. This representation of the FPS Number is the short form representation. The long form representations are translated to a 12 digit equivalent with a 20000 prefix.

        i. A = 0,

        ii. B = 1,

        iii. C = 2,

        iv. D = 3,

        v. E = 4,

        vi. F = 5,

        vii. G = 6,

        viii. H = 7,

        ix. I = 8, and

        x. No letter (non alpha) = 9.

        xi. Note: When printing Non Alpha file numbers as part of the barcode, the “9” must be replaced by a blank (i.e. space character).

3. For consolidations, involving two (2) or more Refugee records, the following ordinal numbering scheme is to be used from lowest to highest: (M)

a. 330008xxxx,

b. 330001xxxx, and

c. Thus, the 330008 is always the lowest, the oldest, of the numbering sequence and then the numbering sequence would follow the “normal” ordinal numbering.

13.3.2 DATABASE VOLUMES

1. The following identifies the data conversion volumes for AFIS, IMM, VSS, Transcoders and ELMO. (I)

   a. AFIS/IMM: refer to Annex B, Section 3.6, Table 5 – Data Volumes for AFIS/IMM data conversion volumes;

   b. VSS: There are expected to be approximately sixty thousand (60,000) Verification (VER) NIST packets/Transactions and approximately 1 million (1,000,000) VSS sets of prints on file that were submitted through AFIS by the end of 2017;

   c. Transcoders: The volume of data on the Transcoders will vary depending on the size of the remote agency. It is estimated that that the larger Transcoder sites will have 1000 Ten Print records, 1000 Latent records and Transcoder log files with 30,000 entries. It is estimated that that the smaller Transcoder sites will have 50 Ten Print records, 50 Latent records and Transcoder log files with 10,000 entries. Seventy-five percent (75%) of the sites are considered small. Each site has less than 25 users; and

   d. ELMO: The ELMO database has approximately 120,000 images, with 80% Latent images and 20% Object shots. Refer to Annex E – LCMC requirements for additional details on the ELMO database and note that the database is directly dependent on the number of images.

13.4 Ten Print (TP) Additional Requirements

1. The Contractor shall add descriptors to the ten print file as required by their Entire AFIS renewal solution. (M)

2. The Contractor shall search each newly added ten print set to the existing sets filed in the AFIS renewal solution database to identify Subjects filed more than once (i.e. under two (2) different subjects or file numbers). (M)

3. The Contractor shall ensure that the Technical Authority is provided with at least two (2) weeks to review and approve the process for carrying out the cleanup of these multiple filings. (M)

4. The Contractor shall ensure that a process is defined and implemented to carry out the cleanup where duplicates and other discrepancies are found. (M)

13.5 Unsolved Latent File (ULF) Additional Requirements

1. The Contractor shall search each newly added ULF entry against the Ten Print file to identify any highly probable hits. (M)
2. The Contractor shall enable the RCMP to verify these highly probable hits. (M)
3. The Contractor shall ensure that the RCMP Technical Authority is provided with at least two (2) weeks to review and approve the process for carrying out the cleanup of these latent hits. (M)
4. The Contractor shall ensure that a process is defined and implemented to carry out the cleanup where latent hit to ten print and discrepancies are found. (M)
5. The Contractor shall identify ULF entries that belong to the same case/image (same minutiae). (M)
6. ULF entries with the same minutia for the same case/image must not be converted. The first or oldest occurrence on the duplicate ULF entry must be retained. (M)
7. Duplicate ULF entries that belong to the same images with different minutiae, even if they belong to the same case must be converted and retained. (M)
8. ULF entries belonging to different cases must be converted and retained. (M)
9. The Contractor shall ensure that a process is defined and implemented to handle any ULF conversion anomalies in an effective and efficient manner. A mechanism to allow the RCMP Latent technician to identify, investigate and approve/reject each anomaly will be established by the Contractor. (M)

13.6 Data Conversion Approach

1. The Contractor will follow the data conversion guidelines outlined in this section. (I)
2. The RCMP will provide: (I)
   a. A small amount of Government-provided space, in the RCMP HQ complex in Ottawa or alternate Ontario conversion site, for Contractor personnel and equipment, determined by the RCMP for data conversion activities; and
   b. Network connectivity for the Contractor’s devices and SAN storage for the data conversion in a secure area of the RCMP/SSC network infrastructure.
3. The Contractor must obtain approval from the RCMP, in writing, for any additional requests for anything else required by the Contractor for data conversion. (M)
4. The Contractor shall provide all of the equipment and personnel to conduct the necessary conversion operations. (M)
5. RCMP information is sensitive and must be meticulously safeguarded by the Contractor. The Contractor shall implement controls to safeguard against unauthorized disclosure, modification, access, use, destruction, or delay in service, of all information and services provided pursuant to this contract. (M)

6. Conversion Records: (M)

    a. The Contractor shall create and maintain accurate, up-to-date records, in digital form, of conversion information for each image converted, unsolved latent, NIST packet, or any other data converted as part of the conversion activities.

    b. The Contractor’s conversion records shall be sufficiently detailed to provide a complete audit trail of each item converted, identifying each device or user used in the process, records not converted and the reason.

    c. All conversion records shall be readily accessible, within 24 hours, to the RCMP.

    d. Upon completion of the conversion, all conversion records, including audit/log files shall be turned over to the RCMP.

13.7 Data Conversion Audit Trail

1. The Contractor shall create and maintain detailed automated records that will provide a full and complete audit trail of control, image-quality, and tracking information on each converted item. These and any other similar records shall be readily accessible to authorized RCMP personnel for review and audit. At a minimum, the audit record maintained for each item converted shall contain the following information: (M)

    a. Transaction Control Number (TCN);

    b. DCN;

    c. File number

    d. Subject ID, where applicable;

    e. Latent file number, where applicable;

    f. Latent ID, where applicable;

    g. Latent image ID, where applicable;

    h. Type of Transaction Code;

    i. Date and time the TCN was assigned;

    j. Previous TCN (if applicable); and

    k. Previous DCN (if applicable);

2. The Contractor shall back up the complete file at least once a day. (M)

3. The Contractor shall maintain an up-to-date backup copy of the complete file. (M)

4. The Contractor shall maintain the Conversion Audit Trail for the life of the AFIS contract. (M)

5. The Contractor shall provide a complete electronic copy of the file, and the hardware and software necessary to access it, to the RCMP within thirty (30) calendar days of the end of the last AFIS conversion activity. (M)

6. The Contractor shall maintain a cumulative accounting of data converted. The accounting must be adequate to identify situations where a second or subsequent electronic record is being prepared for a particular fingerprint image. The Contractor shall institute controls to investigate these cases. No second or subsequent record shall be submitted unless supported by a valid rationale (e.g. directed rescan). RCMP approval is required for all subsequent submissions. (M)

7. The Contractor shall maintain backups of software applications and conversion records in a fashion that will support full and timely recovery of system capabilities in the event of an unplanned outage. These copies must be stored in a manner to ensure no single event can affect both the system and the backups. (M)

13.8 Operational Readiness

1. The Contractor shall include in the Site Acceptance Test Plan (SATP) all the details concerning who, when, where and how the various conversions will be tested. (M)

2. The Contractor shall integrate and test its production system with the converted data in accordance with its approved SATP. (M)

3. Prior to the start of any conversion testing, the Contractor shall conduct a complete pre-production test of all functional aspects of the portion of the Entire AFIS renewal solution for which the data was converted. The Contractor shall demonstrate that the entire system is fully operational, end-to-end prior to acceptance testing by the RCMP. (M)

4. The Contractor shall be responsible for correcting any errors and reprocessing the conversion as many times as required to achieve the correct conversion result based on RCMP analysis of the converted data and the requirements stated throughout this SOW and its accompanying document. (M)

13.9 Quality Control / Quality Assurance

1. The Contractor shall implement a comprehensive Quality Control / Quality Assurance (QC/QA) program commensurate with the goals of the conversion and the critical fingerprint identification mission of the RCMP that the integrity of the RCMP’s fingerprint data is of the utmost importance. (M)

2. The Contractor shall take the necessary steps and implement the necessary audits, reviews, tests, inspections, appropriate procedures, and related QC/QA measures to ensure that each request for conversion services produced by the Contractor meets or exceeds the requirements stated throughout this SOW and its accompanying documents. (M)

3. The Contractor shall apply rigorous QC/QA measures in the following areas, and in other areas deemed by the Contractor as critical to the success of the conversions: (M)

    a. Establishing and maintaining the integrity of the subject ID, TCN, DCN, file numbers or other primary keys and the data associated with them throughout the conversion processes;

b. Ensuring the security of conversion operations; and

c. Have reports that ensure everything was converted properly and discrepancy reports for any data not converting as expected.

d. Ensure legacy data (e.g. Latent file number) that does not follow the RTID numbering scheme are properly converted and are fully usable after the conversion by any part of the Entire AFIS renewal solution that requires it.

14. DOCUMENTATION REQUIREMENTS

14.1 Purpose

1. The Contractor must provide comprehensive documentation including architecture diagrams, design documents (e.g. System Design Document (SDD), preliminary ARIP with completed Requirements Traceability Matrix (RTM), screen capture examples) and any other documentation that clearly demonstrates that the Contractor's proposed solution satisfies the requirements stated throughout this SOW and its accompanying documents. (M)

2. The preliminary ARIP must be provided to demonstrate that the Contractor understands the requirements and explains how the Contractor's solution will be effectively and efficiently implemented. (M)

3. The Contractor must also deliver all the other documentation identified throughout this SOW and its accompanying documents as part of the deliverables required to satisfy the overall requirements. (M)

15. OVERALL DELIVERABLES PLAN AND SCHEDULE

15.1 Overview

1. This section identifies the Contractor major deliverables and describes the content of the deliverables that must be completed as part of this SOW. (M)
2. Expected RCMP deliverables are also listed to allow the Contractor to be aware of these deliverables and ensure they are included in the master schedule with any required dependencies. (I)
3. Any additional deliverables that the Contractor considers important for the successful completion of this SOW must be identified by the Contractor and indicate any RCMP activity related to the additional deliverables. (M)
4. Any additional deliverables that the Contractor requires from the RCMP must be identified. RCMP must approve any changes to the list of deliverables identified in the following schedule table (Subsection 15.2 below). (M)
5. The overall schedule will consider each key area and create a plan that identifies the relationship between each set of components that will be renewed. Any dependencies between components must be identified and an optimized plan that eliminates or minimizes repeating the same steps or tests must be developed. The schedule must correlate to each key area of change and the Basis of Payment. The table in Appendix G, Evaluation Plan and Criteria, might assist with presenting this correlation. The schedule must allow related key areas to be isolated that will allow portions of this SOW to be executed through to completion separately from other key areas. (M)
6. All documents created or updated to complete the deliverables must use RCMP approved office applications. The RCMP approved office applications are Microsoft Office (Word, PowerPoint, Excel, Visio, Project and Access), Version 2010/2013. All documents must be fully editable so they can be updated by the RCMP as part of ongoing future maintenance. Should the Contractor wish to submit documents in other softcopy formats, this must be expressly authorized by the RCMP Technical Authority. (M)

15.2 Contract Deliverables Requirements List (CDRL) Scheduling of Deliverables

1. The following table identifies the deliverables, responsibility for completion, initial delivery date, revision time period and final deliverable dates. (I)
2. The time estimates, identified in the table, are preferred by the RCMP. (R)

3. They are provided to indicate timeframes that initially correspond with RCMP schedules which will be considered in the Master Contract Schedule. The approved Master SOW Schedule, created by RCMP, will identify the agreed to delivery dates for all deliverables. (I)

4. The Deliverable Item Description (DID) refers to the detailed descriptions of each deliverable; which follows the table in this section. The Contractor can, if desired, combine the common deliverables for each key area into one document to minimize repetition. If the Contractor chooses to combine a deliverable, then each key area must be separately sectioned such that each key area can be easily reviewed, updated and correlated to the Basis of Payment. (M)

5. The Implementation Steps and information required for the Change Order (CO) process will be according to the Chief Information Office (CIO) Sector's Change Management policy as referenced in the Maintainability subsection of this SOW. (M)

6. Note: All dates in Table 15-1 below are calendar dates. The *RCMP Review* column represents business days. (I)

Table 15-1: Schedule of Deliverables

No	Description	DID No	Responsible	Initial Delivery Date	RCMP Review	Updated	Final Delivery Date
				Project Management			
1.	Master Contract Schedule (MCS)	PM-01	RCMP / the Contractor	10 days after Contract Award (CA)	5 days	After Contractor review and agreement	10 days after review and agreement
2.	Progress Review Meetings (PRM)	PM-03	RCMP	Semi-monthly	N/A	N/A	3 days after PRM for Minutes and Action List
3.	AFIS Renewal Implementation Plan (ARIP)	ARI-01	the Contractor	With proposal	5	30 days after CA	5 days after RCMP review
4.	Requirements Traceability Matrix (RTM) provided in RFP & completed by the	AT-01	the Contractor	RTM only with proposal, for RCMP use, to validate compliance to AFIS	TBD	For use with ATP/SATP to verify implementation satisfies all	As depicted in PM-01 Gantt Chart

Table 15-1: Schedule of Deliverables

No	Description	DID No	Responsible	Initial Delivery Date	RCMP Review	Updated	Final Delivery Date
	Contractor			Renewal RFP requirements		requirements	
5.	Acceptance Test Plan (ATP)	AT-01	the Contractor	As depicted in PM-01	5 days	After RCMP review	As depicted in PM-01 Gantt Chart
6.	Acceptance Test Report (ATR)	AT-02	the Contractor	As depicted in PM-01	5 days	After RCMP review	As depicted in PM-01 Gantt Chart
7.	System Design Documentation (SDD)	CM-01	the Contractor	With proposal, for RCMP use, to validate compliance to AFIS Renewal RFP requirements	TBD	For use with ATP to verify implementation satisfies all requirements	As depicted in PM-01 Gantt Chart
8.	Data Conversion Strategy & Plan Document	N/A	the Contractor	With proposal, for RCMP use, to validate compliance to AFIS Renewal RFP requirements	TBD	For use and agreement with RCMP on the final data conversion process	As depicted in PM-01 Gantt Chart
9.	Project Documentation • Systems Engineering Management Plan; • Quality Assurance Plan; • Requirements Management Plan; • Configuration Management Plan; • Risk Management	N/A	the Contractor	With proposal, for RCMP use, to validate compliance to AFIS Renewal RFP requirements	TBD	For continued understanding of how the Contractor's solution operates in the RCMP/SSC infrastructure	As depicted in PM-01 Gantt Chart

Table 15-1: Schedule of Deliverables

No	Description	DID No	Responsible	Initial Delivery Date	RCMP Review	Updated	Final Delivery Date
	Plan; • Problem Resolution Plan • Document Management; and • Subcontractor Management Plan						
10.	AFIS & VSS Recovery Plan and Strategy	N/A	the Contractor	With proposal, for RCMP use, to validate compliance to AFIS Renewal RFP requirements	TBD	For continued understanding of how the Contractor's solution operates in the RCMP/SSC infrastructure	As depicted in PM-01 Gantt Chart
11.	AFIS & VSS Operational Procedures	N/A	the Contractor	TBD	N/A	N/A	As depicted in PM-01 Gantt Chart
				All other deliverables			
12.	Delivery of Bill Of Materials (BOM)	N/A	the Contractor	TBD	N/A	N/A	As depicted in PM-01 Gantt Chart
13.	Delivery of hardware	N/A	the Contractor	As depicted in PM-01	5 days	N/A	As depicted in PM-01 Gantt Chart
14.	Site Acceptance Test Plan	AT-03	the Contractor	As depicted in PM-01	5 days	After RCMP review	As depicted in PM-01 Gantt Chart
15.	Site Acceptance Test Report	AT-04	the Contractor	As depicted in PM-01	5 days	After RCMP review	As depicted in PM-01 Gantt Chart

Table 15-1: Schedule of Deliverables

No	Description	DID No	Responsible	Initial Delivery Date	RCMP Review	Updated	Final Delivery Date
16.	Implementation Steps & information required for CO Process	CM Process[1]	the Contractor	As depicted in PM-01	5 days	After RCMP Review	As depicted in PM-01 Gantt Chart
17.	CO Creation	CM Process	RCMP	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
18.	Acceptance Testing (Functional)	Using RCMP Test Plans	RCMP	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
19.	QCS Acceptance Testing (Functional & Technical – Load balancing & HA can only be tested in QCS)	Using RCMP Test Plan	RCMP	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
20.	Prod Acceptance Testing (Functional & Technical – Load balancing & HA)	Using RCMP Test Plan	RCMP	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
21.	Ongoing OS & Software Upgrade	OU-01	the Contractor	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
22.	RTID Release Implementation Plan	N/A	RCMP	As depicted in PM-01	N/A	After the Contractor Input	As depicted in PM-01 Gantt Chart
23.	Software and	DO-01	the Contractor	N/A	5 days	After RCMP Review, and after completion	As depicted in PM-

[1] Change Management Process – Refer to Maintainability subsection

Table 15-1: Schedule of Deliverables

No	Description	DID No	Responsible	Initial Delivery Date	RCMP Review	Updated	Final Delivery Date
	Documentation					of Acceptance Testing	01 Gantt Chart
24.	Milestone Payments	N/A	the Contractor/RCMP	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
25.	Final Acceptance	Review DO-01	RCMP	N/A	N/A	N/A	As depicted in PM-01 Gantt Chart
26.	Milestone Payments	N/A	the Contractor/RCMP	As depicted in PM-01	N/A	10% holdback payment	As depicted in PM-01 Gantt Chart

ATTACHMENT A-1 – DELIVERABLES

Deliverable-1 Master Contract Schedule (MCS)

DATA ITEM DESCRIPTION

1. TITLE Master Contract Schedule (MCS)	2. IDENTIFICATION NUMBER PM-01

3. DESCRIPTION/PURPOSE

The MCS document shall detail all activities from CA signing through to final acceptance and handover of the final products to the RCMP Technical Authority.

The RCMP will be responsible for maintaining this deliverable; however, the Contractor must provide all tasks and completion times for the tasks to allow an effective schedule to be completed. Once the baseline schedule has been agreed to, the Contractor will commit to completing the deliverables according to this schedule. Any required changes or additions for inclusion in the baseline version of the MCS must be approved by the RCMP Technical Authority.

4. PREPARATION INSTRUCTIONS

4.1 General. The MCS shall depict the work and schedule associated with the entire scope of the contract.

4.2 Format Requirements. The schedule portion of the MCS shall be presented in Bar (Gantt) chart format. The activities depicted in the chart shall be based on a planned sequence of events with the time estimates, start and end dates for all events precisely calculated. The Contractor may choose the symbols to be used. A legend depicting the meaning of all symbols shall be included on all schedules submitted. Upon approval of the MCS, the schedule symbols shall not be revised unless agreed by the RCMP Technical Authority.

4.3 Content Requirements. The MCS shall depict all contract work including milestones, events and deliverables associated with the SOW. The MCS will have the following features:

a. The MCS shall clearly show the document Title, date produced and version number as applicable;

b. The MCS shall depict the scope of the work to be satisfied under this SOW using the Work Breakdown Structure (WBS) technique. For each element of the WBS, the Contractor shall provide a clear and concise definition on the element scope and associated deliverables;

c. The MCS shall clearly show each of the key areas to be delivered under this SOW, including subordinate shipping, installation and site acceptance

1. TITLE Master Contract Schedule (MCS)	2. IDENTIFICATION NUMBER PM-01

schedules as applicable;

d. The MCS shall depict the start and end dates including interdependencies of the various tasks, events and milestones to be accomplished under this SOW;

e. The MCS shall identify, as required, the schedule for all plans, deliverables and reports, kick-off meetings, progress review meetings, design review meetings, document review by the RCMP Technical Authority, Contractor demonstrations, on-site tests and inspections, installation, migration activities and acceptance and handover as appropriate;

f. The MCS shall clearly indicate the requirements for delivery or preparation of Government Furnished Items, including equipment and facilities, and Government Furnished Information regarding publications and documents;

g. The MCS shall clearly indicate the milestone payments; and

h. The RCMP will baseline the final version of the MCS once agreed to with the Contractor and approved by RCMP. The baseline content shall not be revised without the written consent of the RCMP Technical Authority.

4.4 Copies. Both a hard and soft copy of the MCS can be provided to the Contractor as required.

Deliverable-2 Progress Review Meetings (PRM)

DATA ITEM DESCRIPTION

1. TITLE Progress Review Meetings (PRM)	2. IDENTIFICATION NUMBER PM-03

3. DESCRIPTION/PURPOSE

The PRM shall provide a forum for discussing the status of the work achieved versus work planned by the Contractor for the reporting period. Subject of discussion shall include progress to-date against the baseline plan, upcoming deliverables, Contractor and RCMP expectations, current risks and issues, problem areas and corrective actions that have been initiated to mitigate the identified problems.

4. PREPARATION INSTRUCTIONS

4.1 General. The PRM shall be held twice a month as scheduled by the RCMP.

4.2 Requirements. The RCMP shall host and conduct twice a month status review meetings in accordance with the approved Master Contract Schedule

a. The PRM will be chaired by the RCMP Technical Authority and will normally take place at the RCMP HQ located at 1200 Vanier Parkway in Ottawa.

b. Government representatives for the PRM may include outside consultants and other Contractors providing support services to the SOW.

c. When appropriate due to the distance between the Contractor’s facility and Ottawa, and at the sole discretion of the RCMP Technical Authority, progress review meetings may be conducted using tele/video-conferencing facilities.

d. The RCMP shall be responsible for co-ordinating progress review meetings as follows:

i. co-ordination with the Contractor and Technical Authority;

ii. provide all administrative support;

iii. provide agenda, minutes, schedules, lists, tests, design analysis, problems, solutions and any other pre and post review data as required;

iv. the Contractor must ensure that their qualified Contractor and Sub-Contractor personnel attend the progress review meetings as required;

v. assure and provide evidence that decisions resulting from various progress review meetings, have been implemented where applicable;

vi. maintain files, records and documents of all reviews;

1. TITLE Progress Review Meetings (PRM)	2. IDENTIFICATION NUMBER PM-03

vii. maintain a prioritized Action Item file; and

viii. maintain a Risk Registry that includes the top ten (10) most significant risk elements of the schedule including their probability of occurrence, impact and mitigation strategies.

e. In addition to the formal progress review meetings, RCMP at its sole discretion may call upon the Contractor to provide representation at adhoc meetings. These meetings are intended to address matters of a serious nature that cannot reasonably be delayed until the next scheduled formal progress review meeting.

4.3 Agenda and Minutes of Meetings

a. The RCMP shall produce and deliver agendas for all progress review meetings three (3) days prior to the PRM. All agendas shall be approved by the RCMP Technical Authority prior to the scheduled PRM.

b. The RCMP shall prepare and deliver the Minutes of every meeting including an Action Items list.

c. The RCMP shall append to the Minutes of every meeting a separate Action Item list that includes all Action Items from all meetings and reviews and their status (open, closed, date, update, etc.). It is the RCMP's responsibility to maintain the Action Items list

4.4 Distribution. The RCMP shall distribute electronic copies of the Minutes of the PRM and the Action List to the Contractor and PWGSC three (3) days after the meetings have been held.

Deliverable-3 AFIS Renewal Implementation Plan (ARIP)

DATA ITEM DESCRIPTION

1. TITLE	2. IDENTIFICATION NUMBER
AFIS Renewal Implementation Plan (ARIP)	AR-01

3. DESCRIPTION/PURPOSE

The purpose of the ARIP is to provide the RCMP Technical Authority with a concise document detailing the Contractor's plan for the installation, implementation, integration, conversion, interoperability and set-to-work activities required for the entire scope of work identified in this SOW. The ARIP is a comprehensive strategy and plan that explains in detail how the work identified in this SOW will be completed in the most cost effective and efficient manner while minimizing the impact to RTID test and Production environments. This deliverable establishes the approach that will be used to complete the work in this SOW in an organized manner that can be integrated in the RCMP release activities.
The purpose of the ARIP is to provide a single integrated view of the overall approach for the Contractor's Proposed Solution. The ARIP shall provide clear justification for the sequence of activities that minimizes any disruption to RTID test and/or Production environment operations. RCMP must approve the ARIP prior to the start of any work resulting from this SOW.

4. PREPARATION INSTRUCTIONS

4.1 Format. The ARIP shall be prepared using RCMP approved Office applications, using the headings and sequence listed in this DID, and shall be legible and suitable for reproduction. The document's numbering scheme shall allow reference to all distinct elements of the ARIP (sections of text, figures, diagrams, tables, etc.). All attachments shall be identified and referenced in the text of the document.

4.2 Document Structure. The ARIP must be structured in a manner that easily correlates to the Basis of Payment, each key area and the agreed to schedule maintained by the RCMP. Each key area identified in this SOW must be described in a separate section that allows the effort required to complete each key area to be identified. To ensure the most cost effective and efficient strategy and plan, multiple key areas can be completed together and any cost saving benefits associated with this type of strategy can be identified as justification for combining the activities.

4.3 Content. As a minimum, the ARIP shall address the following areas:

a. Table of Contents. This section shall identify figures, diagrams, tables, annexes, etc.;

b. Scope. This section shall describe the purpose and contents of the document. It shall present an overview of each section of the system architecture. The ARIP shall address all aspects of the work required to complete this SOW

1. TITLE AFIS Renewal Implementation Plan (ARIP)	2. IDENTIFICATION NUMBER AR-01

except the ongoing upgrade activities;

c. Reference Documents. This section shall list all reference documents and any other relevant resources utilised in the development of this strategy and plan;

d. Assumption. Any assumption associated with the strategy and plan must be identified;

e. Executive Summary. This section of the document must provide a high-level description of the AFIS Renewal solution implementation strategy and plan, identify the major tasks required to complete the work in this SOW and key dates related to the completion of significant milestones. This section is intended for management; therefore, it is expected to be 1–3 pages only;

f. Strategy and Plan Overview. This section of the document must provide a high-level description of the overall strategy and plan that will be used to complete the work required for this SOW;

g. Strategy Options. This section shall describe the strategic options considered to complete the work in this SOW in the most cost effective and efficient manner. General factors, which guided and influenced the strategic decisions and the relative priority of factors such as relationship between components, vulnerabilities, the Contractor development time-lines, RCMP release time-lines, cost, reliability, etc., shall be discussed in light of determining factors that resulted in the strategy and plan. This includes rationale, trade-offs and other considerations affecting any strategic decisions. It shall identify and list any security considerations and/or technical complexities of this renewal initiative as required;

h. Implementation Plan. This section shall provide a detailed description of the proposed implementation plan, including a detailed breakdown of how each key area, identified in this SOW, will be implemented. This plan must consider all aspects of each key area as well as RCMP and RTID process and procedures. This description shall include, as a minimum, the following:

i. When, what components will be upgraded;
ii. A table or equivalent showing the entire scope of all components to be upgraded and for each release highlight the components that are included in the release upgrade (refer to list of all the Contractor components section heading below);
iii. Details describing precisely how the implementation will be completed through each test environment and the Production environment including a back out strategy if applicable. For example, specific details identifying when existing IP addresses will be assumed by the new servers or when new IP addresses are required. To ensure effective and efficient use of RTID test environments, it is expected that parallel operations of the new servers will be required to minimize disruption to the RTID testing;
iv. Risk associated with each implementation and the risk mitigation strategy to reduce the risk to an acceptable level;

1. TITLE	2. IDENTIFICATION NUMBER
AFIS Renewal Implementation Plan (ARIP)	AR-01

v. RCMP Implementation support required throughout each release, including hardware, software, facilities, resources or any other material required to complete the work;

vi. Impact of each release on RCMP and RTID operations in the test and Production environments;

vii. An explanation of the justification used to determine the implementation plan;

viii. All tools and utilities required to execute the implementation plan; and

ix. Any other information required to present a clear understanding of the implementation plan and the required details that ensure all aspects of the current configuration are propagated to the new and/or upgraded components as required.

h. Component Configurations. All configuration parameters and any other aspects of the Contractor Entire AFIS renewal solution that are required to ensure all new and/or upgraded components are fully operational and collectively satisfy all the requirements in this SOW and its accompanying documents.

s. Risk Assessment / Contingency Plans. The plan shall detail the risks associated with the overall implementation plan. Risks shall be described and quantified (as to their likelihood of occurrence and impact consequences) to the extent possible. Items with higher risk and/or consequence shall be outlined in appropriately greater detail. The plan shall discuss any decisions taken to eliminate risk items. Contingency plans shall outline measures for mitigating any remaining risk items. An overview of risks associated with the implementation of the proposed implementation plan shall be given.

t. Physical and Environmental Conditions. This section shall detail any consideration that must be given to the environment within which the Proposed Solution will operate. This includes any provision for environmental controls in rooms where equipment is located, safety issues, etc.

u. List of all the Contractor Components. This section shall indicate the release that the component replacement/upgrade/reuse will be completed. All Contractor components including all the key configuration aspects of the component with at least the following must be included:

i. Host name,
ii. IP address (not included herein for security reasons),
iii. Function,
iv. Model,
v. CPU,
vi. Memory,
vii. Disk storage available,
viii. Operating System including version and service pack / patch number
ix. End-of-life date,
x. End-of-service date,
xi. Hosted software,

1. TITLE AFIS Renewal Implementation Plan (ARIP)	2. IDENTIFICATION NUMBER AR-01

xii. An indication if SAN is required for the component and if so how much is allocated,

xiii. Release number, and

xiv. Any notes associated with the component.

Note: An example table has been included on the next page. This is meant to provide an example of the how to present this portion of the information required for this document. It is expected that this same table will be used in the Ongoing Upgrade DID OU-01.

v. Glossary. A glossary shall be included containing definitions of all abbreviations, mnemonics, and acronyms used in the design;

w. Miscellaneous. This section shall discuss any additional information that the Contractor deems relevant to the implementation plan; and

x. Attachments. Any sections too large to be included in the main body shall be broken out separately as an attachment and shall be referenced from within the main body of the design.

Attachment A-1: Example Table 1

Hostname & IP	Function	Model	CPU	Memory	Disk Space	Operating System	End-of Life Date (HW/OS)	End of Service Date (HW/OS)	Hosted Software	SAN	Release	Notes
Production Environment												
		IBM p720 8202-E4C	3.0 GHz 8-Core	32 GB	2x300 GB	AIX 7.1 SPO	Not Declared	Not Declared	Oracle 11g TSM 5.3 PowerHA			

Deliverable-4 Acceptance Test Plan (ATP)

DATA ITEM DESCRIPTION

1. TITLE Acceptance Testing – Acceptance Test Plan (ATP)	2. IDENTIFICATION NUMBER AT-01

3. DESCRIPTION/PURPOSE

The Proposed Solution Acceptance Test Plan shall describe the planning and testing that will be undertaken for the Proposed Solution. It shall stipulate the general procedures, terms and conditions governing the planning, preparation and completion of the tests covering the proposed solution submitted for acceptance. The early submission of this plan will give RCMP the opportunity to review the plan and make any required changes/additions.

4. PREPARATION INSTRUCTIONS

4.1 Format Requirements. Each Acceptance Test Plan shall be prepared using RCMP approved Office applications and shall be legible and suitable for reproduction. Pages shall be sequentially numbered. All attachments shall be identified and referenced in the text of the document.

4.2 General. The Acceptance Test Plan shall describe the process of demonstrating the proper operation of the software, hardware and architecture (as applicable), in order to validate the design, implementation, migration and interoperability of the Proposed Solution. The plan shall stipulate the approach and procedures governing the planning, preparation and completion of acceptance testing for the Proposed Solution. The plan shall be based on the Contractor’s test scripts and manual test process. Subsequent to demonstrating the complete integration and proper operation of the Proposed Solution as an integral component of the RCMP Technical Architecture within the MAINT or alternate designated environment, the ATP shall describe the process of conducting performance and capacity tests to demonstrate that the Contractor’s solution satisfies the Proposed Solution Performance Benchmarking Criteria and other technical requirements within the Production environment.

4.3 Content Requirements. As a minimum, the Proposed Solution ATP shall include:

a. Table of Contents. This section shall identify figures, diagrams, tables, annexes, etc.;

b. Scope. This section shall describe the purpose and scope of the document. Where applicable, the portions of the Proposed Solution to which the document applies shall be identified and a brief overview of that portion of the Proposed Solution shall be provided. The general testing philosophy to be employed in validating the Proposed Solution shall be explained (e.g. formal inspection, integration testing, migration testing, etc.). This section shall discuss features to be tested and not tested, giving justification for any features of Proposed Solution that will not be tested;

c. Reference Documents. This section shall acknowledge any reference documents having a relationship or used in the creation of this plan;

d. Overall Test Objectives. This section shall specify the major objectives for each Proposed Solution acceptance testing in three (3) phases. Objectives shall be stated in terms of satisfying Proposed Solution specifications. A unified set of objectives for the entire ATP shall be established. The objectives of the first phase of testing should include accepting that the system components as delivered have been installed, interconnected, operate to RCMP's specifications and satisfy all requirements stated throughout the SOW and its accompanying documents for the scope of ATP in the MAINT or alternate designated environment. The objectives of the second phase of testing should be acceptance of proof that the system as delivered meets RCMP's performance and capacity requirements. Types of testing to be conducted shall include, but not be limited to, integration, boundary, stress, error, capacity, performance and failover testing. Failover testing shall be included in the test objectives in order to confirm that the system components respond to any problems that may necessitate a change in processing in either environment as well as Backup and Recovery testing that ensures 100% recoverability for any of the Proposed Solution components. Testing of all required tools or interfaces to be used within and/or between the Proposed Solution or any other impacted applications and systems shall also be specified. The third phase of testing will include the RCMP's acceptance testing and Production environment of the Proposed Solution;

e. Test Schedule. This section shall present timelines for testing. It shall give estimates for the dates of testing and the time duration allotted to each test;

f. Test Facilities, Personnel and Special Equipment. This section shall detail the test facilities, equipment and personnel necessary to effect the testing described in the Proposed Solution's ATP. This shall include, but is not limited to, the following:

i. Identification of test equipment and software required to conduct testing of the Proposed Solution, including the use of any commercial or proprietary testing tools;

ii. Identification of facilities required to support the test effort (including Contractor and Government facilities);

iii. Personnel support requirements necessary for the conduct of testing, including discussion of the organisational structure of the testing team(s) and responsibilities of test team members. Involvement of Government personnel, where required, shall also be specified; and

iv. Description of the analysis tools and/or techniques to be used to assess test results and make pass/fail determinations;

g. Software and Hardware Configuration Details and Diagram. This section shall detail the configuration of software and hardware that will be at the RCMP Primary and DR sites and/or each environment as applicable that will be used for testing of the Proposed Solution. Topology diagrams shall be used to show the physical configuration of the hardware and logical configuration diagrams shall show the configuration / partitions of the software. The diagrams shall be accompanied by a textual description of same;

h. General Test Procedures. This section shall discuss any general prerequisite actions that must be taken prior to commencement of testing. This includes, but is not limited to, validation of the Proposed Solution applicable hardware and software configuration prior to the start of testing. In cases where identical pre-test activities are required for a multiple of tests, description of these activities may be broken out as a separate block of text (e.g. as a pre-amble or appendix to the general test procedures section) and shall be referenced by each test procedure. This section shall briefly describe each test to be conducted. The following information shall be provided for each test:

i. The purpose of the test, including a description of any parameters to be measured. Any interdependencies with other tests shall be noted;

ii. The Requirements Traceability Matrix (RTM) provided in the RFP, shall be completed by the Contractor to describe or demonstrate how the Contractor's Proposed Solution satisfies all the requirements identified in this SOW and its accompanying documents for the scope of ATP. The Contractor must provide either a single ATP that includes an RTM for all requirements identified in this SOW and its accompanying documents or multiple RTMs that collectively include all requirements identified in this SOW and its accompanying documents;

iii. Test acceptance criteria for each test shall be provided. Pass/fail criteria for each test shall be outlined and cross-referenced to the Proposed Solution capability;

iv. Identification of test scripts to be used in performing the test described in the general test procedures section;

v. Procedures to be taken in the event of a test failure (e.g. retest, rework, etc.); and

vi. Instructions for recording test results on a designated form (e.g. checklists, test log, etc.) shall be included in the Test Plan. Predefined forms such as checklists or test logs shall be included as appendices or attachments;

i. Test Scripts. All test scripts called for by the Test Plan shall be included in the document. Each test should be presented as a discrete sub-section within the document such that it can be referenced by external documents. Test scripts shall include all necessary inputs and expected outputs;

j. Test Analysis. Where applicable, the procedures for analysing test results in order to determine a pass/fail status for a test shall be presented. Tests requiring post-testing analysis of test data shall be noted;

k. Acceptance Test Products. This section shall describe the products of the testing activities including their format and structure (e.g. checklists, test logs, test analyses, etc.). These products will serve as a permanent record of the testing activity;

l. Miscellaneous. This section shall include any additional information that the Contractor believes is relevant to the testing activity but is not addressed elsewhere in the DID; and

m. Attachments. The attachments contain material that is too bulky or detailed to be placed in the main body text. Attachments are to be referenced in the main body of the text where the information applies.

Deliverable-5 Acceptance Test Report (ATR)

DATA ITEM DESCRIPTION

1. TITLE Acceptance Testing – Acceptance Test Report (ATR)	2. IDENTIFICATION NUMBER AT-02

3. DESCRIPTION/PURPOSE

The Proposed Solution Acceptance Test Report (ATR) shall record the results of tests performed on the Proposed Solution in accordance with the Test Plan outlined in Proposed Solution ATP. This report shall either verify to the RCMP Technical Authority that the system software, hardware, directory, configuration and migration strategy have passed all the required acceptance tests and meet the requirements as stated in the contract, or have failed the acceptance tests with reasons for failure.

4. PREPARATION INSTRUCTIONS

4.1 Format Requirements. The Proposed Solution ATR shall be prepared using RCMP approved Office applications and shall be legible and suitable for reproduction. Pages shall be sequentially numbered. All attachments shall be identified and referenced in the text of the document.

4.2 General. The purpose of this report is to provide the RCMP Technical Authority and the Contractor with a permanent record of the results of the acceptance tests performed on the system software, hardware, configuration and migration. This DID contains the format and content requirements for the test report.

4.3 Content Requirements. As a minimum, the Proposed Solution ATR shall include:

a. Table of Contents. This section shall identify figures, diagrams, tables, annexes, etc.;

b. Scope. This section shall describe the purpose and scope of the document. The Platform ATR shall provide a comprehensive summary of testing done according to DID AT-01, for the purpose of validating the complete Proposed Solution as an integral component of the RCMP Technical Architecture within the MAINT or alternate designated environment as well as within RCMP's Production infrastructure. A review of the general testing philosophy laid out in the Proposed Solution ATP shall be given along with a brief discussion of the contents of this Proposed Solution ATR;

c. Related Documents. This section shall provide references including applicable and related documents;

d. System Configuration Diagrams. A detail system configuration as-tested shall be

1. TITLE Acceptance Testing – Acceptance Test Report (ATR)	2. IDENTIFICATION NUMBER AT-02

included, with any discrepancies from the configuration described in the ATR noted and reasons for the discrepancies given;

e. Overview of Test Results. An overview of the results of the testing process shall be given, noting the general types of testing that were done. An assessment of the success of each type of testing shall be given, along with any significant problems or test failures. Any incidents of rework or re-testing shall be noted;

f. Detailed Test Results. This section shall present the results of each test, to be preceded by an overview of the test, its objectives, acceptance criteria, and pass/fail determination. This section shall be divided into the following paragraphs to describe the results of each test covered by this report:

i. Test Name and scope of test as outlined in DID AT-01;

ii. Test Summary including acceptance criteria;

iii. Where applicable, any post-test analysis of test results required to determine a pass/fail condition shall be presented;

iv. Test Results, specifically a pass/fail determination, shall be presented for each test. Results recorded for each step of the test cases during testing shall be presented. Discrepancies from expected test results encountered during the execution of the test case shall be described. Information (e.g. memory dumps, record of registers, display diagrams, etc.) that may help to isolate and correct the cause of any discrepancies shall be included or referenced. The test director may speculate as to the specific cause of each discrepancy and suggest diagnostic and corrective measures;

v. Test Records kept during testing shall present a record of all events relevant to test preparation, performance, analysis and interpretation of test results. This subparagraph shall include the following information where relevant:

a) The Test Date(s) and Test Location(s);

b) Description of hardware and software test configurations;

c) Personnel involved in the testing and their role or responsibility in the test process noted;

d) Problems encountered and the specific step(s) of the test procedures associated with the problem, including the number of times an individual step in a procedure had to be repeated and the outcome of each attempt; and

e) Backup points or test steps where tests were resumed; and

1. TITLE Acceptance Testing – Acceptance Test Report (ATR)	2. IDENTIFICATION NUMBER AT-02

vi. Any deviations from the original test procedure shall be presented in detail (e.g. substitution of required equipment, changes to support software, procedural steps not followed and schedule deviations). The rationale for each deviation and the impact on the validity of the test shall be provided;

g. Test Logs/Checklists. Any test logs, checklists, test analyses, or other documentation produced as a result of the acceptance testing shall be included and cross-referenced to the test or tests for which it was produced;

h. Evaluation and Recommendations. Based on an analysis of the test results, the test report shall make a recommendation for system acceptance/rejection based on the results of acceptance tests described above. This section shall be divided into the following sub-sections:

i. Evaluation. This section shall provide an overall analysis of the capabilities of the item demonstrated by the test results in this report. The analysis shall identify any remaining deficiencies, limitations or constraints that were detected by the test performed. Engineering Change Proposals may be used to supplement deficiency information. For each deficiency, limitation or constraint, the analysis shall provide a recommended solution; and

ii. Recommended Improvements. This section shall provide any recommended improvements in the design or operation of the system. The impact of implementing, and the impact of not implementing, the recommendations shall be outlined. Any assumptions, which were used to formulate the recommended improvement should be provided;
Note: The RCMP Technical Authority has responsibility for accepting/rejecting the system based on his/her determining if the test results support the system satisfying the Proposed Solution requirements as stated in this SOW and its accompanying documents.

i. Miscellaneous. This section shall include any additional information resulting from the acceptance testing that the Contractor deems relevant to the test report; and

j. Attachments. Any sections of the document that are too large to incorporate into the main body of the document shall be included as attachments and referenced as such.

Deliverable-6 Site Acceptance Test Plan (SATP)

DATA ITEM DESCRIPTION

1. TITLE Acceptance Testing – Site Acceptance Test Plan (SATP)	2. IDENTIFICATION NUMBER AT-03

3. DESCRIPTION/PURPOSE

The Proposed Solution Site Acceptance Test Plan shall describe the planning that shall be undertaken to demonstrate the complete integration and proper operation of the Proposed Solution in each site/environment. It shall stipulate the general procedures, terms and conditions governing the planning, preparation and completion of acceptance tests covering the site/environment submitted for acceptance. Also, it shall describe how the timing of interruptions and the interruption to existing facilities will be carried out. The early submission of the Site Acceptance Test Plan will give the RCMP the opportunity to review the plan and make any required changes/additions.

Unless otherwise agreed to in writing by the RCMP, a separate SATP must be completed for each release based on the strategy and plan developed in the approved ARIP. The ARIP establishes the approach that will be used to complete the work in this SOW in an organized manner that can be integrated in the RCMP release activities. The SATPs provide the detailed implementation steps and testing that will be completed in each site/environment that ensures the replacements/upgrades/reuse are effectively implemented with all the quality controls required to successfully complete the work in this SOW.

4. PREPARATION INSTRUCTIONS

4.1 Format Requirements. The Proposed Solution SATP shall be prepared using RCMP approved Office applications and shall be legible and suitable for reproduction. Pages shall be sequentially numbered. All attachments shall be identified and referenced in the text of the document.

4.2 General. The Proposed Solution SATP shall describe the process of demonstrating the proper operation of the software, hardware and architecture in order to validate the complete integration, migration, interoperability of the Proposed Solution in order to qualify the specified Proposed Solution site/environment for acceptance. The plan shall describe the approach and procedures governing the planning, preparation and completion of acceptance testing for the site/environment submitted for acceptance. The plan shall be based on the Contractor's testing and RCMP testing. The SATP shall include each test environment and the RCMP Primary and DR installation of the Proposed Solution and shall be tailored to reflect unique characteristics of each site and/or environment.

4.3 Content Requirements. As a minimum, the SATP shall include:

1. TITLE Acceptance Testing – Site Acceptance Test Plan (SATP)	2. IDENTIFICATION NUMBER AT-03

a. Table of Contents. This section shall identify figures, diagrams, tables, annexes, etc.;

b. Scope. This section shall describe the purpose and scope of the document. Where applicable, the portions of the system to which the document applies shall be identified and a brief overview of the portion of the system shall be provided. Features of the Proposed Solution that will not be tested should be discussed and rationale for not testing presented. This section shall specify the major objectives for the site/environment acceptance test. Objectives shall be stated in terms of satisfying the system specifications. A unified set of objectives for the entire site/environment acceptance test process shall be established;

c. Reference Documents. This section shall acknowledge any reference documents having a bearing on the Proposed Solution implementation at the site/environment in question;

d. Overall Test Objectives. This section shall specify the major objectives for site/environment testing. Objectives shall be stated in terms of satisfying the scope of the release. A unified set of objectives for the entire SATP shall be established. At a minimum, the objectives must include verifying components as delivered have been installed, interconnected and operate to RCMP's specifications in the environment, proof that the system as delivered meets RCMP's performance and capacity requirements, integration, SNMP reporting, error, HA testing, AV Scanning and WSUS testing as required. HA testing shall be included in the test objectives in order to confirm that the system components respond to any problems that may necessitate a change in processing in any environment with HA capabilities. Testing of all required tools or interfaces to be used within and/or between the Proposed Solution or any other impacted applications and systems shall also be specified;

e. Site/Environment. This section shall uniquely identify the site/environment for which the specified acceptance testing is to be performed. An overview of the site topology shall be given. Rather than repeat excessive amounts of information from other documents, reference for further detail on architecture or site topology may be made to other DIDs as appropriate (e.g. AR-01 AFIS Renewal Implementation Plan);

f. Acceptance Testing Program Management. This section shall describe the planning associated with acceptance testing activities;

g. Test Schedule. This section shall present timelines for testing. It shall give estimates for the dates of testing and the time duration allotted to each test;

h. Implementation Steps. The detailed implementation steps required to effectively implement the solution in each site/environment must be identified;

1. TITLE	2. IDENTIFICATION NUMBER
Acceptance Testing – Site Acceptance Test Plan (SATP)	AT-03

i. Site Facilities, Personnel and Special Equipment. This section shall detail the site/environment facilities, equipment and personnel necessary to effect the testing described by the SATP. This shall include, but is not limited to, the following:

   i. Identification of general and site/environment specific equipment and software that constitutes the site/environment's Proposed Solution to be tested;

   ii. Identification of any hardware and software required to conduct testing of the Proposed Solution, including the use of any commercial or proprietary testing tools;

   iii. Identification of any other facilities required to support the test effort (including Contractor and Government facilities);

   iv. Personnel support requirements necessary for the conduct of testing, including discussion of the organisational structure of the testing team(s) and responsibilities of test team members. Involvement of Government personnel, where required, shall also be specified; and

   v. Description of any test analysis tools or techniques which will be used to analyse test data for the purpose of determining a pass/fail verdict for one or more tests;

j. Pre-test System Configuration. The plan shall discuss the required software, hardware and configurations necessary prior to the commencement of testing:

   i. Software Configuration. This section shall discuss the required configuration of software, which shall be present on target systems prior to commencement of testing. This section shall outline the steps necessary to ensure that this configuration is verified by testing personnel prior to commencement of testing;

   ii. Hardware Configuration. This section shall discuss the required configuration of hardware, which shall be in place on target systems prior to commencement of testing. This section shall outline the steps necessary to ensure that this configuration is verified by testing personnel prior to commencement of testing; and

   iii. Directory Configuration. This section shall describe the directory configuration that must be present on the target system(s) prior to commencement of testing;

k. Test Objectives. This section shall discuss the general and specific test objectives that pertain to the site/environment undergoing test, including any parameters that are to be measured. Types of testing to be employed shall be

1. TITLE	2. IDENTIFICATION NUMBER
Acceptance Testing – Site Acceptance Test Plan (SATP)	AT-03

discussed (e.g. boundary testing, error testing and/or stress testing);

l. General Test Descriptions. This section shall give a general overview of the tests to be performed, along with their respective acceptance criteria. Test acceptance criteria, where applicable, shall be drawn from the Proposed Solution requirements as stated in this SOW and its accompanying documents. This shall include, but is not limited to, the following:

i. The purpose of the test, including a description of any parameters to be measured. Any interdependencies with other tests shall be noted;

ii. The Requirements Traceability Matrix (RTM) provided in the RFP, shall be completed by the Contractor to describe or demonstrate how the Contractor's Proposed Solution satisfies all the requirements identified in this SOW and its accompanying documents for the scope of SATP;

iii. Test acceptance criteria for each test shall be provided. Pass/fail criteria for each test shall be outlined and cross-referenced to the Proposed Solution capability;

iv. Identification of test scripts to be used in performing the test described in the general test procedures section;

v. Procedures to be taken in the event of a test failure (e.g. retest, rework, etc.); and

vi. Instructions for recording test results on a designated form (e.g. checklists, test log, etc.) shall be included in the Test Plan. Predefined forms such as checklists or test logs shall be included as appendices or attachments;

m. Environmental and Electrical Test Conditions. Any unique or relevant points concerning the conditions under which testing will occur shall be discussed;

n. Test Scripts. The test scripts to be used for testing shall be included in the Test Plan. The test scripts shall be prepared in the Contractor's format. Every discrete action performed during testing by test operators shall be reflected in the test script/procedure. Test scripts shall note all required inputs and actions required of test operators along with all expected test outputs for all relevant test steps;

o. Acceptance Test Products. This section shall summarise the outputs of the acceptance test activities. The format of test logs, test records, checklists, test analyses, etc., shall be outlined in the Site Acceptance Test Plan. Test logs shall contain, as a minimum, the following information:

i. Site/environment identifier uniquely identifying each test location;

ii. Test identifier uniquely identifying each test;

1. TITLE Acceptance Testing – Site Acceptance Test Plan (SATP)	2. IDENTIFICATION NUMBER AT-03

iii. Test date;

iv. Test personnel, including test director, test operator(s), observers, etc.;

v. Test run identifiers for each test run, including indication of test completion, test pass/fail, retest, errors, etc.; and

vi. Comments on testing activities (problems, documentation errors, etc.);

p. Design Parameters and Tolerances. The Test Plan shall discuss design parameters and any key design features that shall receive special testing (stress testing, performance testing, boundary testing and/or error testing, etc.);

q. Interruptions of Services. This section shall describe when and how the interruptions of services will be impacted, the duration of interruptions and the activities done to mitigate the impact of interruptions;

r. Miscellaneous. This section shall include any additional information that the Contractor would like to add to enhance the document and that is not addressed elsewhere in the DID; and

s. Attachments. The attachments shall contain material that is too bulky or detailed to be placed in the main body text. Attachments are to be referenced in the main body of the text where the information applies.

Deliverable-7 Site Acceptance Test Report (SATR)

DATA ITEM DESCRIPTION

1. TITLE Acceptance Testing – Site Acceptance Test Report (SATR)	2. IDENTIFICATION NUMBER AT-04

3. DESCRIPTION/PURPOSE

The Proposed Solution SATR shall record the results of tests performed on the Proposed Solution at the specified site/environment. The SATR shall either verify to the RCMP Technical Authority that the system software, hardware and configuration has passed all the required Site Acceptance Tests and met the requirements as stated in the contract, or have failed the Site Acceptance Tests with reasons for failure. The SATP is used a base to generate the SATR. Using the SATP and recording the results of the test and activities will allow the SATR to be generated.

4. PREPARATION INSTRUCTIONS

4.1 Format Requirements. The Proposed Solution SATR shall be prepared using RCMP approved Office applications and shall be legible and suitable for reproduction. Pages shall be sequentially numbered. All attachments shall be identified and referenced in the text of the document.

4.2 General. The purpose of the Proposed Solution SATR is to provide the RCMP and the Contractor with a permanent record of the results of the acceptance tests performed on the system software, hardware and configuration at a specified site/environment. Test reports shall be produced for each site/environment as a result of Site Acceptance Testing done, in accordance with the Test Plan called for by DID AT-03, Proposed Solution Site Acceptance Test Plan. This DID contains the format and content requirements for the test report.

4.3 Content Requirements. A summary of the content requirements is contained in the following sections:

a. Table of Contents. This section shall identify figures, diagrams, tables, annexes, etc.;

b. Scope. This section shall describe the purpose and scope of the document. The SATR shall provide a comprehensive summary of testing done according to DID AT-03, for the purpose of validating the complete Proposed Solution as an integral component of the RCMP's Production infrastructure. It shall give an overview of the site/environment that was subject to acceptance testing. Where applicable, the portions of the Proposed Solution to which the document applies shall be identified and a brief overview of the portion of the system shall

1. TITLE Acceptance Testing – Site Acceptance Test Report (SATR)	2. IDENTIFICATION NUMBER AT-04

be provided. Features of the Proposed Solution software or system that were not tested should be discussed and rationale for not testing discussed. This section shall specify the major objectives for the site/environment acceptance test. Objectives shall be stated in terms of satisfying the system specifications. A unified set of objectives for the entire site/environment acceptance test program shall be established;

c. Related Documents. This section shall provide references including applicable and related documents. It shall refer to the originating site acceptance Test Plan prepared according to DID AT-03, Proposed Solution Site Acceptance Test Plan;

d. Site/Environment. This section shall identify the specified site/environment, by location and building. This information shall also be included on the front cover of this document;

e. Site/Environment Software / Hardware Configuration Diagrams. This section shall include an overview of the system software and hardware configurations that were in effect at the time of testing. Differences in these configurations from those outlined in the applicable Site Acceptance Test Plan shall be noted, along with reasons for the discrepancies;

f. Test Overview. An overview of the features of the Proposed Solution that were tested shall be given. Reference shall be made to tests called for by the corresponding Site Acceptance Test Plan. Any tests planned in the Site Acceptance Test Plan but not conducted shall be noted and rationale given for the tests not being run;

g. Detailed Test Results. This section shall be divided into the following paragraphs to describe the results of each test covered by this report:

i. Test Name and scope of test as outlined in DID AT-03, Proposed Solution Site Acceptance Test Plan;

ii. Test Summary including test acceptance criteria;

iii. Test Results, specifically a pass/fail determination, shall be presented for each test. Results for each step of the test procedure shall be listed. Discrepancies encountered during the execution of the test case shall be described. Information (e.g. memory dumps, record of registers, display diagrams, etc.) that may help to isolate and correct the cause of any discrepancies shall be included or referenced. The test director may speculate as to the specific cause of each discrepancy and suggest diagnostic and corrective measures;

iv. Test Records shall present a record of all events relevant to test preparation, performance and analysis and interpretation of test results. This section shall include the following information where relevant:

1. TITLE Acceptance Testing – Site Acceptance Test Report (SATR)	2. IDENTIFICATION NUMBER AT-04

a) The Test Date(s) and Test Location(s) of the test;

b) A description of hardware and software test configurations;

c) Personnel involved in the testing and their role or responsibility in the test process noted and their signatures;

d) Problems encountered and the specific step(s) of the test procedures associated with the problem, including the number of times an individual step in a procedure had to be repeated and the outcome of each attempt; and

e) Backup points or test steps where tests were resumed;

v. Any deviations from the original test procedure shall be presented in detail (e.g. substitution of required equipment, changes to support software, procedural steps not followed and schedule deviations). The rationale for each deviation and the impact on the validity of the test shall be provided; and

vi. Any other acceptance test products that were produced during testing (e.g. test logs, test records, checklists, test analyses, etc.) shall be included;

h. <u>Evaluation and Recommendations.</u> This section shall be divided into the following paragraphs:

i. <u>Evaluation.</u> Provide an overall analysis of the capabilities of the item demonstrated by the test results in this report. The analysis shall identify any remaining deficiencies, limitations, or constraints that were detected by the test performed. Engineering Change Proposals may be used to supplement deficiency information. For each deficiency, limitation, or constraint, the analysis shall provide a recommended solution; and

ii. <u>Recommended Improvements.</u> This paragraph shall provide recommended improvements in the design or operation of the system. The impact of implementing, and the impact of not implementing the recommendations shall be outlined. Any assumptions that were used to formulate the recommended improvement should be provided;
Note: The RCMP Technical Authority has responsibility for accepting/rejecting the system based on his/her determining if the test results support the system satisfying the Proposed Solution requirements as stated in this SOW and its accompanying documents.

i. <u>Miscellaneous.</u> This section shall include any additional information that the Contractor deems relevant to enhance the document and that is not addressed elsewhere in the DID; and

j. <u>Attachments.</u> The attachments shall contain material that is too bulky or detailed to be placed in the main body text. Each attachment should be referred to in the main body

1. TITLE Acceptance Testing – Site Acceptance Test Report (SATR)	2. IDENTIFICATION NUMBER AT-04
of the text where the information applies.	

Deliverable-8 System Design Documentation (SDD)

DATA ITEM DESCRIPTION

1. TITLE	2. IDENTIFICATION NUMBER
System Design Documentation (SDD)	CM-01

3. DESCRIPTION/PURPOSE

The Proposed System Design Document (SDD) is the design for the Proposed Solution which results from the Contractor’s review and analysis of the Proposed Solution Requirements and Specifications stated in the SOW and its appendices, the results of test and integration, and review of the various applicable RCMP documents. The purpose of the SDD is to provide a single integrated view of the overall architecture for the Contractor’s Proposed Solution. The SDD shall provide justification for major design decisions. Configuration Items are identified and inter-architecture configuration items to be integrated are identified and described. This SDD deals with the final architecture configuration of the Proposed Solution. Portions of the architecture that relate to the Proposed Solution Management function(s) can be described.

4. PREPARATION INSTRUCTIONS

4.1 Format. The SDD shall be prepared using RCMP approved Office applications, using the headings and sequence listed in this DID, and shall be legible and suitable for reproduction. The document’s numbering scheme shall allow reference to all distinct elements of the design (sections of text, figures, diagrams, tables, etc.). All attachments shall be identified and referenced in the text of the document. The Contractor must update all originally supplied VSS renewal solution design documents to reflect all design changes to date, including the changes resulting from the completion of this SOW. The format of the original VSS renewal solution design document is expected to be followed.

4.2 Content. As a minimum, the SDD shall address the following areas:

a. Table of Contents. This section shall identify figures, diagrams, tables, annexes, etc.;

b. Scope. This section shall describe the purpose and contents of the document. It shall present an overview of each section of the system architecture. The SDD shall address all requirements of the Proposed Solution Specifications stated in this SOW and its appendices;

c. Reference Documents. This section shall list all reference documents and any other relevant resources utilised in the design of the system architecture;

d. Standards and Protocols. All standards and protocols having a bearing on the architecture shall be described and associated with the relevant portion of the architecture;

1. TITLE	2. IDENTIFICATION NUMBER
System Design Documentation (SDD)	CM-01

e. General Design Factors. This section shall describe general design factors, which guided and influenced the design of the system architecture. The relative priority of factors such as system performance, cost, reliability, etc., shall be discussed in light of determining factors that resulted in the architecture favouring any criteria at the expense of another. This includes rationale, trade-offs and other considerations affecting major design decisions. It shall identify and list the functional and technical design requirements (including security considerations), design goals, and technical complexities of the project that influenced trade-off decisions. Influencing factors can include, but are not limited to: architecture, capabilities and constraints of existing RCMP architecture, systems and applications; security considerations; implementation considerations, etc.;

f. General System Architecture Description. An overview of the system architecture shall be provided in this section. This shall include a description of the system architecture at the national and site levels. High-level diagrams shall be used as applicable. The corresponding reference system model that was followed as a basis for design shall be discussed, along with a breakdown of how the system components map against that model (e.g. 2-tier and 3-tier client/server architecture, OSI 7-layer reference model, etc.);

g. Detailed System Architecture. This section shall provide a concise description of the architectural design of the Proposed Solution, including a detailed breakdown of how the system architecture complies with the requirements of the Proposed Solution specifications. This description shall include, as a minimum, the following:

i. system architecture description and diagrams to illustrate the finer details of system and site level architecture. The diagrams shall reflect all discrete components of the Proposed Solution topology, including servers, matchers, routers, gateways, user sites, etc.;

ii. a summary of major design elements of the hardware and software components of the system architecture (purpose, capabilities, significant characteristics, configuration and justification for incorporation). If applicable, this section shall distinguish between re-use of existing resources from the existing environment and new infrastructure components (servers, matchers, etc.) required to implement the design;

iii. all tools and utilities called for in the architecture shall be described in terms of their functions and how these functions support the Proposed Solution requirements;

iv. where conversion tools or utilities are called for in the architecture, a statement of which protocol and content version(s) are supported through the conversion facility and how this exchange will occur in the Proposed Solution architecture shall be provided; and

1. TITLE System Design Documentation (SDD)	2. IDENTIFICATION NUMBER CM-01

v. all information relating to interfaces between the Proposed Solution and other supporting systems (e.g. directory services) or projects;

h. System Components. All discrete components or facilities that make up the Proposed Solution shall be described.

i. Performance. The design shall detail and assess the performance, throughput, and capacity characteristics of the architecture in response to requirements of the Proposed Solution Technical Specifications and Performance Criteria. All performance criteria shall be based on the lowest bandwidth line available for the relevant portion(s) of the system. The design shall outline the hardware and software configurations to be used and explain how the Proposed Solution Technical Specifications and Performance Criteria will be satisfied. Performance, throughput, and capacity metrics shall be detailed for client, server, and network components of the architecture. For each metric, the design shall note the factors that influence the metric (hardware or software). The design shall explain portions of the Proposed Solution architecture for which performance or throughput metrics cannot be measured. It shall list and give justification for those portions of that cannot be subject to the Performance Criteria;

j. Hardware/Software. All Contractor provided hardware and software (e.g. servers, switches, routers, gateways, servers, workstations, etc.) introduced by the system architecture shall be detailed in terms of specifications and function within the architecture. The architecture shall distinguish between Contractor provided hardware/software and pre-existing hardware, software, or facilities at the Proposed Solution sites. Specifications for hardware (e.g. capacity, processors, speed, memory size, etc.) and software (e.g. memory requirements, version number) shall be included;

k. Remote User Access. This section shall detail the design features that are responsive to the requirements of remote system administration (e.g. sites that are geographically remote from the Proposed Solution servers located at the RCMP Primary site);

l. Directory Services. The Contractor shall provide details on how directory services will be integrated into the Proposed Solution in response to the requirements listed in the Proposed Solution Technical Specifications. Use of all directory service products (proprietary or otherwise) shall be described including a clear explanation as to how their functionality maps to the Proposed Solution technical specifications for directory services. Justification for the selection of directory services shall be provided (i.e. contrast the various options available and explain why one is chosen over the other(s)). The design shall describe the synchronisation of the Proposed Solution directory and the RCMP's enterprise X.500 directory (in keeping with the manner in which directory services are implemented) along with any required directory synchronisation tools;

m. Security Plan. This section shall detail the security architecture of the

1. TITLE	2. IDENTIFICATION NUMBER
System Design Documentation (SDD)	CM-01

Proposed Solution. The security plan shall cover the following areas:

i. Security-Related Design Issues. This section shall discuss influences and constraints on the security architecture imposed by technology features and limitations, Proposed Solution requirements, The RCMP security policy, etc. Design decisions relating to security shall be justified in light of these influences and constraints;

ii. Security Architecture Overview. This section shall present a clear description of the design of the security system, including descriptions and diagrams (where applicable) of the national and site-level topologies;

iii. Security Architecture Design. This section shall identify and describe the structure of the security system in terms of its major hardware and software configuration items. This shall encompass issues such as physical security, user logon, system administration security features, etc. The architecture shall provide a detailed description of the access control mechanisms and an example of the administrative files or screen images of administrative screens; and

iv. Public Key Infrastructure (PKI). This section shall describe how the Proposed Solution shall interface to the RCMP PKI. This section shall explain any Proposed Solution related issues concerning access to public key certificates and the synchronisation of user login and authentication process with the PKI;

n. Interoperability. This section shall provide an overview of the ability of the Proposed Solution architecture to interface and operate with the current heterogeneous environment, with the RCMP directory services and other impacted network services and applications throughout and after the Proposed Solution deployment period;

o. Scalability and Component Upgrade. The design shall detail the Proposed Solution architecture's capacity for expandability (scalability) and ability to absorb future enhancements and upgrades to software and hardware components with minimal impact to the user community. Quantitative figures (metrics) shall be given concerning all scalability aspects;

p. Reliability. The design shall describe how the proposed system architecture meets the reliability requirements of the Proposed Solution. The design shall discuss expected reliability parameters for the hardware and software components of the system. The design will discuss any other reliability factors for the system hardware and software that the Contractor feels are relevant but not explicitly stated in the Technical Specifications;

q. Availability and Maintainability. An assessment of the Proposed Solution's implementation of availability and maintainability requirements shall be given. System availability shall be detailed in terms of:

1. TITLE	2. IDENTIFICATION NUMBER
System Design Documentation (SDD)	CM-01

i. ability of system to meet continuous service requirements as per Proposed Solution technical specifications;

ii. expected durations of system downtime periods required for any maintenance activities (i.e. hardware repairs, system restores from backup, etc.); and

iii. level of service available during administrative procedures (e.g. replication and synchronisation of directories, etc.) along with expected time required for such activities;

r. Survivability. This section shall give an appreciation of the survivability aspects of the architecture. This includes, but is not limited to, any redundancy features and an assessment of the Proposed Solution’s ability to absorb degradation of architecture components (server component failures, server outages, router failures, etc.);

y. Risk Assessment/Contingency Plans. The plan shall detail the risks associated with the overall system design. Risks shall be described and quantified (as to their likelihood of occurrence and impact consequences) to the extent possible. Items with higher risk and/or consequence shall be outlined in appropriately greater detail. The plan shall discuss any design decisions taken to eliminate risk items. Contingency plans shall outline measures for mitigating any remaining risk items within the architecture. An overview of risks associated with the implementation of the Proposed Solution shall be given;

z. Physical and Environmental Conditions. This section shall detail any consideration that must be given to the environment within which the Proposed Solution will operate. This includes any provision for environmental controls in rooms where equipment is located, safety issues, etc.;

aa. Glossary. A glossary shall be included containing definitions of all abbreviations, mnemonics, and acronyms used in the design;

bb. Miscellaneous. This section shall discuss any additional information that the Contractor deems relevant to the system architecture; and

cc. Attachments. Any sections too large to be included in the main body shall be broken out separately as an attachment and shall be referenced from within the main body of the design.

Deliverable-9 Ongoing OS and Software Upgrades (OOSU)

DATA ITEM DESCRIPTION

1. TITLE Ongoing OS & Software Upgrade (OOSU)	2. IDENTIFICATION NUMBER OU-01

3. DESCRIPTION/PURPOSE

The purpose of the Ongoing OS and Software Upgrade (OOSU) document is to provide the RCMP Technical Authority with a document detailing the ongoing upgrade activities and maintain an up-to-date record of the configuration management of the test and Production servers, workstations and Transcoder components. This existing document must be maintained to provide the latest configuration for every Contractor component, as well as maintain an historical record of all upgrades completed day forward under this SOW using RCMP products. Records, Documents and Information Management System (RDIMS), or its RCMP replacement, is available to maintain the historical changes for a document. The RCMP expects the Contractor to use RDIMS to maintain this historical record of upgrades. RDIMS together with track changes on the document will allow the latest configuration to be identified as well as the historical record of changes with each upgrade. If the Contractor wants to use an alternative method, it must be approved by the RCMP.

Note 1: There is no requirement for architecture diagrams or architecture descriptions in this document. Its purpose is to record ongoing support. Any upgrades that require architectural changes would be completed under a separate Task Authorization (TA).

Note 2: A separate RTID Release Implementation Plan will always be developed for any upgrade; therefore, this document does not need to include any specific implementation details.

4. PREPARATION INSTRUCTIONS

4.1 Format. The existing OOSU shall be updated for each upgrade completed by the Contractor using RCMP approved Office applications and shall be legible and suitable for reproduction. All attachments shall be identified and referenced in the text of the document.

4.2 Content. As a minimum, the OOSU shall detail the following:

a. Record of Amendments. This section shall maintain a list the amendments to the document, identifying at a minimum, the date of change, person responsible for the change, brief description of the change and the version number of the document;

b. Table of Contents. This section shall identify figures, diagrams, tables, annexes, etc.;

1. TITLE	2. IDENTIFICATION NUMBER
Ongoing OS & Software Upgrade (OOSU)	OU-01

c. Scope. This section shall describe the purpose and contents of the document. It shall present an overview of each section of the OOSU;

d. Upgrade Purpose. This section shall describe the purpose of the specific upgrade being completed. This section must describe sufficient detail that allows the reader to clearly understand the specific upgrade without reviewing the details of each component;

e. Reference Documents. This section shall list all reference documents and any other relevant resources utilised in the design of the system architecture;

f. Assumptions. This section shall list all relevant assumptions associated with the document;

g. Special Considerations. This section shall list any special consideration associated with the upgrade. For example:

i. any tools or utilities required to complete the upgrade, include a description of why it is required and how it is used; or
ii. any conversion required with an explanation of why and how it was completed.

h. Upgrade Impact. This section shall describe the impact of the upgrade with at least the following considered:

i. Capacity;
ii. Performance;
iii. Maintainability;
iv. Availability;
v. Manageability;
vi. Scalability; and
vii. Survivability.

i. Upgrade Issues. This section shall describe any issues that will, or potentially could have, an impact to the operation of the Contractor components with at least the following considered:

i. Describe the issue;
ii. Describe the probability of occurrence and expected or potential impact; and
iii. Propose a mitigation plan to avoid/minimize interruptions to systems in the production and each of the test environments.

j. List of all the Contractor Components. This section shall list all the Contractor components including all the key configuration aspects of the component with at least the following included:

i. Host name;
ii. IP address (not included herein for security reasons);

1. TITLE Ongoing OS & Software Upgrade (OOSU)	2. IDENTIFICATION NUMBER OU-01

iii. Function;
iv. Model;
v. CPU;
vi. Memory;
vii. Disk storage available;
viii. Operating System including version and service pack / patch number;
ix. End-of-life date;
x. End-of-service date;
xi. Hosted software;
xii. An indication if SAN is required for the component and if so how much is allocated;
xiii. Date of the last upgrade;
xiv. Vulnerabilities resolved – This is expected to be a reference to a separate document that identifies the specific vulnerabilities that have been resolved. If this upgrade is simply a regular maintenance upgrade or an update of the anti-virus DAT file, then it must be stated herein;
xv. Issues, concerns and/or notes associated with the upgrade; and
xvi. Any impact on the capacity or performance as a result of the upgrade.

Note: An example table format has been included on the next page. This is meant to provide an example of the how to maintain this portion of the information required for this document.

Attachment A-1: Example Table 2

Hostname	Function	Model	CPU	Memory	Disk Space	Operating System	End-of Life Date (HW/OS)	End of Service Date (HW/OS)	Hosted Software	SAN	Last Update	Vulnerabilities Resolved	Issues / Concerns / Notes	Capacity / Performance Impact
Production Environment														
		IBM p720 8202-E4C	3.0 GHz 8-Core	32 GB	2x300 GB	AIX 7.1 SPO	Not Declared	Not Declared	Oracle 11g TSM 5.3 PowerHA					

Deliverable-10 Software and Documentation

DATA ITEM DESCRIPTION

1. TITLE Software and Documentation	2. IDENTIFICATION NUMBER DO-01

3. DESCRIPTION/PURPOSE

The purpose of the software and documentation is to provide a certified and approved version of the software and documentation for the Proposed Solution after Final Acceptance of the system. This includes all software and documentation related to all aspects of the Contractor's proposed solution; including Operating System, system administration and user guide documentation not specifically identified as a deliverable; however, it forms part of the documentation for the overall solution.

4. PREPARATION INSTRUCTIONS

4.1 Format. The software and documentation shall be prepared using RCMP approved Office applications and shall be legible and suitable for reproduction. Pages shall be sequentially numbered. All attachments shall be identified and referenced in the text of the document. Since the Contractor's proposed solution is based on a COTS product, it is expected that existing Contractor documents will be modified to satisfy this deliverable.

4.2 Content. It is the Contractor's responsibility to include the software and documentation required to describe all design aspects of the proposed solution with sufficient detailed that clearly explains to RCMP how all requirements are satisfied.

ATTACHMENT A-2 – LIST OF DEFINITIONS

The purpose of this attachment is to define the terminology used within this Statement of Work.

Attachment A-2: List of Definitions	
Term	**Definition**
AFIS ICD	The AFIS ICD contains the NIST transactions that are used to communicate with the AFIS. This interface standard allows the RCMP to maintain independence from the proprietary AFIS yet communicate all of the necessary information required to request fingerprint searches.
AFIS Subject ID	A unique identifier assigned by the RTID AFIS system to a Subject (person) enabling the linkage of all fingerprints, regardless of file type, to the Subject.
Audit Log	A list of predetermined system related events that need to record when, where and why, whatever happened and by whom, to ensure an historical record of those events are captured. Refer audit requirements in this SOW and its accompanying documents.
Auto Certification	An RTID AFIS configuration that allows for a Ten Print “lights out” or automatic confirmation of a fingerprint match of a search fingerprint to an existing subject on RTID AFIS.
Biographic Data	This term refers to alpha and numeric type data contained within a Submission. Examples include; Name, Date of Birth, Sex.
Candidate	A candidate is a potential identification provided by the AFIS. This term is closely linked to respondent. Refer to the respondent definition for more clarity on this term.
Configurable Parameter	Refers to a parameter that can be adjusted by a User who possesses the appropriate level of authorization. Configurable parameters typically refer to a system defined function, such as an Service Level Agreement (SLA), retention period for files, queue size, number of candidates, etc.
Contributor	An authorized agency that submits requests for service to CCRTIS. Examples of requests for service include Criminal Retain (CAR-Y), Criminal Inquiry (CAR-N), Civil (MAP), Refugee (REF) and Immigration (IMM) submissions.
CPIC (Query)	A CPIC query retrieve criminal record related data from CPIC.
Date-Time	This term refers to the combination of a date and time; where the time should default to 00:00:00, indicating the start of a particular day, if the time has not been specifically identified.
Entire AFIS Renewal Solution	This term refers to everything to be provided by the Contractor to satisfy all the requirements stated through this SOW and its accompanying documents.

Attachment A-2: List of Definitions

Term	Definition
Fingerprint Biometric Data	This term refers to fingerprint images contained within a Submission.
Immigration File (IID) Number (Immigration Identification Number)	The Immigration Identification File Number is the unique key generated by the RCMP under which Immigration data is stored within the RCMP. An IID Number, once purged, will never be reused.
Interface Control Document (ICD)	A specification for interfacing with a (legacy, internal or external) subsystem, system or service. ICDs and related documents that are relevant to the Immigration include: • Internal ICDs (e.g. AFIS ICD and Internal Subsystem (IIS) ICD; • External ICDs (e.g. NPS-NIST ICDs for external contributors); and • ICD Transformation and FBI Conversion Specification.
Miss	A “Miss” or “Misses” refers to a scenario where an identification was missed and for a TP transaction another Subject Id was created for the same individual. When these Misses are later identified, they must be consolidated to ensure only one Subject Id exists for one individual.
NPS NIST ICD	The term National Police Services NPS NIST ICD is used to refer to the External NPS-NIST ICD versions that include the Types Of Transactions (TOTs) that RTID supports.
One to One (1:1) Verification	For purposes of verification at a CBSA Port of Entry, this term denotes the comparison of submitted fingerprints to the corresponding subject’s enrolled fingerprints (referenced by the IID Number) stored on the Immigration (IMM) Subject File and IMM Subject Repository.
ORI	The Originating Agency Identifier (ORI) is a seven (7) digit alpha-numeric identifier used by the system to identify an agency that has submitted a submission to the RCMP.
OSR	Operating Statistics and Reporting Code (OSR). Crime type code.
Respondent	A respondent is a subject or potential subject identified by file number. This term is closely related to candidate. For example, a Ten Print Search Request (TPRI) could include respondent to be searched based on a prior name search that potentially identified a subject file number. Alternatively, a one to many search could identify candidates for identification and after verification/certification one or more respondents could be included in the Ten Print Request Response (TPREI).

Attachment A-2: List of Definitions

Term	Definition
RTID AFIS	The existing RTID AFIS solution includes all AFIS and VSS capabilities; as well as AFIS workstations, printers, cameras and scanners used by RCMP staff for all types of fingerprint analysis; and remote Transcoders which are used by major Canadian Police agencies to complete crime scene fingerprint investigations.
Subject	An identified individual with a unique Subject Id (retained) or an incoming submission with unique set of prints (non-retained).
Subject File	This term refers to a specific file associated with a unique Subject Id.
Submission	A request for service initiated by an external contributor to add, retrieve, amend, remove or search for information held in the RCMP National Fingerprint Repository. A submission may contain one or more transactions. For Example; an Enrolment contains the following transactions: • an IMM; • if applicable an Error Transaction (ERRT); • an Acknowledgement Transaction (ACKT); and a Search Response (SRE).
Submission Data	This term refers to the data created as a result of processing each submission. Examples include; Activity Log Entries, Status Histories and Internal Transactions to RTID AFIS as well as other Subsystems etc.
System Availability	Availability is defined as the system’s ability to receive and acknowledge a Submission. Availability is measured on a monthly basis. It does not apply to peripherals such as workstations or printers; unless all workstations are unavailable.
Transaction	This terms refers to a defined interaction within a submission. An exchange of information with the system or a subsystem.
Type-14 ID Flats	The term Type-14 record is an NPS NIST ICD defined standard format that can be used to share fingerprint ID Flat images which are acquired by a subject placing their fingers on a fingerprint capture device without the need to roll the finger to capture a complete fingerprint image. These types of images are sometimes referred to as “slaps”. The RCMP definition or standard for “ID Flats” requires 1 to 3 of the following images: • Right Four (4) Fingers; • Left Four (4) Fingers; and/or • Two (2) Thumbs.
User(s)	The term User or Users refers to CCRTIS Authorized User(s) that have been provided access to the function or User Interface referred to in these requirements.

Attachment A-2: List of Definitions

Term	Definition
Verification	Comparing a candidate fingerprint/palm print to a search fingerprint/palm print.
Verification Repository	This term refers to the IMM biometric fingerprint and encoding (minutiae) created and retained for Verification (VSS) purposes. It also includes the image data and biographical information.
Verification Subsystem	The term Verification Subsystem is defined as all the components required to fully support all Verification Subsystem requirements.
Work in Progress	The term Work in Progress (WIP) is defined as the time period from receipt of the submission to Completion of Service plus a buffer period. The Buffer Period is a system configurable number of days based on the submission type. For example an IMM enrolment may be kept for 24 hours (current value) after completion of service prior to data clean-up.
WIP Data	The term WIP Data is the data that is produced as a by-product of related processing. Examples include; Name Search Iterations, Name Search Results, File Status Query Results, Activity Log entries, etc.

ATTACHMENT A-3 – LIST OF ACRONYMS

Attachment A-3: List of Acronyms

Acronym	**Definition**
ACKI	Acknowledgement Internal
ACKL	Acknowledgement Latent
ACKT	Acknowledgement Transaction
ADS	Active Document Storage (database, repository and server)
AFIS	Automated Fingerprint Identification System
AFN	Subject File identifier (The identifier of a given individual)
AIMS	Administrative Information Management System
AKA	Also Known As
AMP	Amputated (or bandaged – record layout field name)
AN	Alphanumeric (character type)
ANS	Alphanumeric Special (character type)
ANSD	Alphanumeric, Special, Date (character type)
ANSI	American National Standards Institute
ARIP	AFIS Renewal Implementation Plan
ASCII	American Standard Code for Information Interchange (standard and text file format)
ATP	Acceptance Test Plan
ATR	Acceptance Test Report
ATS	Anonymous Ten Print Search (transaction)
AV	Anti-Virus
BBS	Biometric Business Solutions (part of CCRTIS)
BOM	Bill Of Materials
BSO	Border Services Officer
CA	Contract Award
CAR N	Criminal Inquiry (Tenprint submission) Non-Retain
CARI	Criminal Internal (Ten Print submission)
CARY	Criminal (Ten Print submission) Retain
CBSA	Canada Border Services Agency
CCRTIS	Canadian Criminal Real Time Identification Services
CCTV	Closed-Circuit Television

Attachment A-3: List of Acronyms

Acronym	Definition
CDRL	Contract Deliverables Requirement List
CHS	Criminal History System
CIC	Citizenship and Immigration Canada (a.k.a. Immigration Refugee Citizenship Canada - IRCC)
CIO	Chief Information Officer
CISCP	French acronym for CPSIC
CJIM	Criminal Justice Information Modernization (A system that stores electronic submissions and electronic charge dispositions from the contributor.)
CLC	Central Latent Client (replaced RAFIAS)
CO	Change Orders
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf system
CPIC	Canadian Police Information Center
CPSIC	Canadian Police Services Information Centre
CPU	Central Processing Unit
CR	Change Record
CREMMS	Criminal Records Entry, Maintenance, and Monitoring System (An RTID subsystem for entry and maintenance of criminal records)
CRIFI	Criminal Record Information Fetch Internal (transaction)
CRS	Criminal Record Synopsis
CRUD	Create, Read, Update and Delete
CSA	Canadian Standards Association
CSE	Communication Security Establishment
CSI	Crime Scene Investigation
CSV	Comma-Separated Value (file format)
CV	Calculated Value
CSR	Contractor Status Report
DAT	Data files for AV scanning software
DB	Database
DCN	Document Control Number
DEVTEST	Development/Test
DF	Direct File

Attachment A-3: List of Acronyms

Acronym	Definition
DID	Data Item Description
DNA	Deoxyribonucleic Acid
DNS	Domain Name Service
DOB	Date of Birth
DOC	Document
DOCID	Document Identifier
DR	Disaster Recovery
DSB	Departmental Security Branch
DVD	Digital Video Disc
EBTS	Electronic Biometric Transmission Specification (The FBI's implementation of the ANSI/NIST Standard for the Interchange of Fingerprint Images. (i.e., the updated EFTS will be renamed EBTS)
EFCD	Electronic Fingerprint Capture Device
EFS	Extended Feature Set
EFTS	Electronic Fingerprint Transmission Specification
EIA	Enterprise Information Architecture
ELMO	Electronic Latent Management Operations (client application, Microsoft Structured Query Language (SQL) Server database, server and system)
EMPPI	Internal Employee Enrolment Purge Request
ePo	(McAfee AV) ePolicy Orchestrator
ERRI	Image Request Error Internal
ERRIN	Internal Error Transaction
ERRL	Error Latent
ERRT	Error Transaction
ERRV	Error on Verification Transaction
EST	Eastern Standard Time
ETL	Extract Transform Load
FBI	Federal Bureau of Investigation
FIS	Forensic Identification Services
FK	Foreign Key (42574)
FOLI	Folio (information request) Internal (transaction)
FOLRI	Folio Response Internal

Attachment A-3: List of Acronyms

Acronym	Definition
FP	Fingerprint (image)
FPS	Fingerprint Section (FPS number is a number that uniquely identifies a criminal in Canada. The primary key under which criminal data is stored in a CR2 or CRS file. Fingerprint images and minutiae are currently stored by FPS number)
FRC	Facial Recognition Capability
FTP	File Transfer Protocol
GB	Gigabyte
GC	Government of Canada
GFE	Government Furnished Equipment
GH	Gigahertz
GUI	Graphical User Interface
HA	High Availability
HBA	Host Bus Adapter
HDS	Hitachi Data Systems
HQ	Headquarters
HRMIS	Human Resources Management Information System
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol – Secure (over Secure Sockets Layer)
HVSP	Hitachi Data Systems (HDS) Virtual Storage Platform
HW	Hardware
IAFIS	Integrated Automated Fingerprint Identification System (FBI)
IBM	International Business Machines
ICD	Interface Control Document
ICMP	Internet Control Message Protocol
ID	Identifier
IEC	Immigration External Contributor
IEEE	Institute for Electrical and Electronic Engineering
IGMP	Internet Group Management Protocol
IID	Immigration Identification File Number
IIS	Immigration Information Sharing (Specifically the Canada-U.S. Immigration Information Sharing project.)

Attachment A-3: List of Acronyms

Acronym	Definition
ILRI	Image List Retrieval Internal
ILRRI	Image List Retrieval Response Internal
IMA	Immigration Amend Transaction
IMAR	Immigration Amend Response
IMM	Immigration Enrolment Transaction
IMP	Immigration Purge Transaction
IMPI	Immigration Purge – Internal
IMPR	Immigration Purge Response
INCITS	International Committee for Information Technology Standards
IP	Internet Protocol
IPSec	Internet Protocol Security
IQS	Image Quality Specification
IRCC	Immigration, Refugee and Citizenship Canada (a.k.a. Citizenship and Immigration Canada - CIC)
IRQ	Image Request
IRQI	Image Request Internal
IRR	Image Request Response
IRRI	Image Request Response Internal
ISF	IDENT Section File number
IT	Information Technology
ITL	Information Technology Laboratory (National Institute of Standards and Technology – U.S.)
JPEG	Joint Photographic Experts Group
LABI	Label Internal (type of transaction)
LAN	Local Area Network
LB	Load Balancing
LCANI	Latent Cancellation Internal (transaction)
LCLO	Latent Closure
LCLOI	Latent Closure Internal
LCMC	Latent Case Management Capability
LDAP	Lightweight Directory Access Protocol
LFFS	Latent Fingerprint Features Search

Attachment A-3: List of Acronyms

Acronym	Definition
LFFSI	Latent Fingerprint Features Search Internal
LFS	Legacy Latent Fingerprint Images Submission (replaced by LFSNS)
LFSI	Latent Fingerprint (image) Submission Internal
LFSNS	Latent Fingerprint Images Submission (replaced LFS)
LFSNSI	Latent Fingerprint Submission (Internal)
LFSRD	Latent (fingerprint) Features Search Response Disposition
LFSRDI	Latent (finger print) Features Search Response Disposition Internal
LSR	Latent Submission Results
LSRFI	Latent Submission Result Foreign Internal
LSRI	Latent Submission Result Internal
LSRLI	Latent to ULF Search Response
LT	Latent
LTCI	Latent Commit Internal
MAINT	Maintenance (environment)
MAP	Miscellaneous Applicant
MAPI	Miscellaneous Applicant (MAP) Internal
MB	Megabyte
MCS	Master Contract Schedule
MOC	Memorandum of Cooperation
MOSPF	Multicast Open Shortest Path First
MPLS	Multiprotocol Label Switching
NAH	Number of background records that are Anticipated to be Hit
NAT	Network Address Translation
NCH	Number of correct hits
NCO/IC	Non-Commissioned Officer / In Charge
NFIQ	NIST Fingerprint Image Quality
NFM	Number of False Matches
NGI	Next Generation Identification (FBI AFIS)
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMSO	National Master Standing Offer

Attachment A-3: List of Acronyms

Acronym	Definition
NNS	National Police Services – National Institute of Standards and Technology (NPS-NIST) Server (RCMP – Transaction and workflow manager for RTID)
NNS ICD	NPS-NIST External ICD
NOTF	Name of Official Taking Fingerprints
NPS	National Police Service
NPSNet	National Police Services Network
NSP	National Security Posture
NTP	Network Time Protocol (42561)
NVN	Non Valid Number
OA	Office Automation
OCR	Optical Character Recognition
OIC	Officer in Charge
ON	Ontario
OOSU	Ongoing Operating System (OS) and Software Upgrade
OPP	Ontario Provincial Police
OPS	Operational Support
ORI	Originator ORI (CPIC unique identified)
OS	Operating System
OSI	Open Systems Interconnection (reference model)
OSPF	Open Shortest Path First
OSR	Operational Statistics and Reporting (code)
PC	Personal Computer
PCS	Paper Conversion Subsystem (Subsystem of RTID that is used to convert paper based fingerprint forms into electronic submissions.)
PDF	Portable Document Format (Adobe)
PK	Primary Key (a unique identifier for a group of related information, normally associated with a row in a database table. This may be based on one or more identifiers known to the business, or may be an internally generated integer managed by a DBMS)
PKI	Public Key Infrastructure (technology or directory server)
PL	Palm Latent
PN	Position Number
POE	Port of Entry

Attachment A-3: List of Acronyms

Acronym	Definition
POP	Post Office Protocol (e.g. POP3)
PP	Palm Print
PR	Primary
PRM	Progress Review Meetings
PROD	Production (environment)
PS	Police Service
PSPC	Public Service and Procurement Canada (AKA PWGSC)
PURI	Purge Request Internal
PWGSC	Public Works and Government Services Canada (GC) (AKA PSPC)
QA	Quality Assurance
QC	Quality Control
QCNI	Query Criminal Name Index
QCS	Quality Control Section
RAFIAS	Regional Automated Fingerprint Identification Access System
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RBAC	Role Based Access Controls
RCMP	Royal Canadian Mounted Police
RDIMS	Records, Documents and Information Management System
REF	The Refugee submission type prepared by CBSA/CIC/RCMP when enrolling a Refugee subject in the RTID system
REFI	Refugee submission (Ten Print) Internal
RFI	Request For Information
RFP	Request For Proposal
RMS	Records Management System
RNSC	Remote Network Search Coordinator
ROSS	RCMP Office Support System
RPC	Remote Procedure Call
RTID	Real Time Identification (system)
RTM	Requirements Traceability Matrix
SACSS	Security Administration and Client Support Section

Attachment A-3: List of Acronyms

Acronym	Definition
SAKMS	Secure Applications and Key Management Service
SAN	Storage Area Network (e.g. SAN space or a SAN disk array)
SATP	Site Acceptance Test Plan
SATR	Site Acceptance Test Report
SCNet	Secure Channel Network (GC)
SDD	System Design Documentation
SDLC	System Development Life Cycle
SDM	Service Desk Manager
SDPPM	Systems Delivery and Project Portfolio Management (as of April 2015, this is the new name for “Major Projects Directory”)
SE	System Engineering
SFFRI	Subject File Fetch Response Internal
SIP	Site Installation Plan
SLA	Service Level Agreement
SME	Subject Matter Expert
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPOC	Single Point of Contact
SPVM	Service de Police de la Ville de Montréal
SQ	Sûreté du Québec
SQL	Structured Query Language
SRCL	Security Requirements Check List
SRE	Search Response
SREI	Search Response Internal
SRL	Search Response Latent
SRLI	Search Response Latent Internal
SRMI	Search Response Message Internal
SRV	Verification Search Response
SSC	Shared Services Canada

Attachment A-3: List of Acronyms

Acronym	Definition
SSH	Secure Shell (program and protocol)
SSL	Secure Sockets Layer (authentication, encryption technology and protocol)
STI	Status Transaction
SYSTEST	System Test (environment)
TA	Task Authorization
TBD	To Be Determined
TCN	Transaction Control Number
TOT	Type of Transaction
TP	Ten Print
TPF	Ten Print File
TPAI	Ten Print Amend Internal
TPARI	Ten Print Amend Response Internal
TPCI	Ten Print Commit Internal
TPCNI	Ten Print Consolidation transaction Internal
TPCNRI	Ten Print Consolidation Response Internal
TPDI	Ten-Print Delete Request Internal
TPDRI	Ten Print Delete Response Internal
TPF	Ten Print File
TPQCI	Ten Print Quality Control Response Internal
TPREI	Ten Print Request Response Internal
TPRI	Ten Print Search Request Internal
TPSEI	Ten Print Direct Scan Internal
TPULI	Ten Print to Unsolved Latent Internal
TPWDI	Ten Print WIP Delete Request Internal
TPWDRI	Ten Print WIP Delete Response Internal
TR	Temporary Resident
TRB	Temporary Resident Biometrics (a.k.a. Immigration)
TSC	Time Stamp Counter (ELMO term)
TSM	Tivoli Storage Manager
TT	Transaction Time
TTC	Transaction Time Coefficients

Attachment A-3: List of Acronyms

Acronym	Definition
UI	User Interface
ULA	Unsolved Latent Amend
ULAI	Unsolved Latent Amend Internal
ULARI	Unsolved Latent Amend Response Internal
ULD	Unsolved Latent Delete
ULDI	Unsolved Latent Delete Internal
ULDR	Unsolved Latent Delete Response
ULDRI	Unsolved Latent Delete Response Internal
ULE	Unsolved Latent Enrolment
ULEI	Unsolved Latent Enrolment Internal
ULER	Unsolved Latent Enrolment Retrieval
ULERI	Unsolved Latent Enrolment Retrieval Internal
ULF	Unsolved Latent File
ULR	Unsolved Latent Retrieval
ULRI	Unsolved Latent Retrieval Internal
ULRR	Unsolved Latent Retrieval Response
ULRRI	Unsolved Latent Retrieval Response Internal
US	United States
USA	United States of America
USB	Universal Serial Bus
USSRL	US Search Response Latent
UTP	Unshielded Twisted Pair
VA	Vulnerability Assessments
VAC	Visa Application Center
VARCHAR	Variable length Character
VER	Verification Submission
VIP	Virtual IP (address)
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSP	Virtual Storage Platform
VSS	Verification Subsystem

Attachment A-3: List of Acronyms

Acronym	Definition
WBS	Work Breakdown Structure
WI	Work Item – RCMP Software/Solution Incident Report
WIP	Work in Progress
WSDL	Web Services Description Language
WSQ	Wavelets Scalar Quantization (a compression algorithm that uses wavelet technology)
WSUS	Windows Server Update Services
XML	eXtensible Mark-up Language
YO	Young Offender (ADS flag)
YOB	Year of Birth
YP	Young Person