MAJOR PROJECTS DIRECTORATE

APPENDIX A

STATEMENT OF WORK

RTID AFIS RENEWAL

Last Updated Date: 2015-10-04
Status: Draft
WBS: REB-11
Version: 0.4
RDIMS Document No.: 42071
Classification: Protected A

RECORD OF AMENDMENTS

Version No.	RDIMS Ver.	Date	Comments	Author (s)

TABLE OF CONTENTS

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.
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.
3. The requirements contained in this SOW and its accompanying documents will be used by Canada to select a Contractor that will renew the existing AFIS and its related subsystems.
4. 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.

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 capabities required to satisfy all requirements stated in this SOW and its accompanying documents.
2. These requirements include the replacement/upgrade/re-use of all components and subsystems in the Production environment and three test environments.
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.
4. This requirement includes the support and maintenance of all environments in a manner that provides a secure operating environment within the RCMP/Shared Services Canada (SSC) infrastructure.
5. This requirement includes user training on the User Interfaces (UIs) for Entire AFIS renewal solution as well as ongoing support and maintenance of all AFIS components.

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.

1.3 DOCUMENT ORGANIZATION

1. This document is organized in manner that allows the overall high level requirements to be understood before describing the detailed requirements for each key area that must be provided by the Contractor. Unless otherwise stated, all the high level requirements and the detailed requirements identified throughout this SOW and its annexes and attachments must be satisfied by the Contractor.

2. The following describes the document organization in point form:
    a. This Appendix A describes the:
        i. Compliancy documents that must be supported by the Contractor's proposed solution,
        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 that must be delivered by the Contractor,
        v. High level technical requirements that must be satisfied by the Contractor's proposed solution,
        vi. On-going support requirements that must be provided, and
        vii. All the deliverables that must 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 Latent Case Management Capability;
    g. Annex F lists all Government Furnished Equipment (GFE) available for use by the Contractor;
    h. Annex G list the workflows for the NNS processing that requires interaction with AFIS; and
    i. Annex H describes the evaluation criteria that will be used to select the successful bidder.

1.4 DOCUMENT PURPOSE

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

1.5 INTENDED AUDIENCE

1. The intended audience for this document are the prospective AFIS Contractors that are interested and capable of providing the products and services necessary to satisfy all the requirements stated in this SOW and its accompanying documents.

1.6 COMPLIANCY STANDARDS AND REFERENCE DOCUMENTS

1.6.1 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 1.6.1.

    - AFIS Internal Subsystem Interface Control Documents (a.k.a. AFIS ICD) (rev. 1.0 H), (RDIMS #42236, 42237, 42562);
    - Web Service Transport Description Document (RDIMS #18413)[1] ;
    - TRB NPS-NIST ICD 2.1.0 / 2.1.1 for External Contributors, (a.k.a. TRB ICD) (RDIMS #35766, #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);

[1] These documents are considered Protected A documents and they will be made available on the Industry Day after the interested Vendors sign an non-disclosure agreement.

- 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;

- EBTS Type-9; and

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

1.6.2 REFERENCE DOCUMENTS

1. The following documents were used to develop this SOW:

   - TRB Verification RCMP Web Service-Front End Technical Design (RDIMS #38422) ;

1.6.3 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:

   http://infoweb.rcmp-grc.gc.ca/cio/so/ops/oirs/private/cm/cm.htm

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

1.7 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 RFP. The Contractor must supply all goods and services required to satisfy all the requirements stated in this SOW and its accompanying documents.

1.7.1 THE CONTRACTOR

1.7.1.1 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 satisfy the requirements stated throughout this SOW and its accompanying documents; and comply with server/workstation security requirements of the RCMP for all environments:
   a. Development/Test (DEVTEST),
   b. Quality Control Systest (QCS),
   c. Maintenance/Certification (MAINT),
   d. Production (PROD), and
   e. Disaster Recovery (DR)

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.
3. Testing to ensure all the Contractor functionality is fully operational between all Contractor components; and between the Contractor components and the RCMP/RTID components.
4. Performance testing that verifies the renewal satisfies all the capacity and performance requirements stated in this SOW and its accompanying documents.
5. Training on all User Interface (UI) aspects of all Contractor components.
6. Conversion of all existing AFIS and its subsystems data to a form usable by the Contractor's proposed solution such that all requirements in this SOW and its accompanying documents are satisfied.
7. FRC capabilities supporting the requirements stated in this SOW and its accompanying documents.
8. Management of the Contractor's personnel, tasks and processes that ensure the timely, effective and efficient completion of all work identified in this SOW and its accompanying documents.
9. All other deliverables and services required by the Contractor to satisfy the requirements stated in this SOW and its accompanying documents.

1.7.1.2 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.
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.
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.
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 six (6) months of contract award unless specifically identified herein. The Production environment includes both the Primary (PR) and Disaster Recovery (DR) sites implementation. Refer to sub-section 1.12 (Timeliness of Deliverables) for additional information concerning scheduling the work to be completed through this SOW.

1.7.1.3 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 SOW 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.

1.7.1.4 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. 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 (GOC) to evaluate the proposed solution.

1.7.1.5 Benchmark Testing

1. Benchmark testing must be completed in North America (i.e. Canada or continental U.S.A.) at a location proposed by the Contractor and agreed to by the RCMP.
2. The benchmarks will take approximately one week per Bidder with 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.
3. The Contractor is responsible for providing and configuring a benchmark configuration of the proposed solution that will used in the benchmark testing.
4. The Contractor will be provided with the benchmark data set and the first test must start 30 working days from the next business day.
5. The Bidders will submit their detailed Benchmark Procedures to the RTID PWGSC Procurement Officer no later than fifteen (15) working days prior the scheduled benchmark. The Bidder's Benchmark Test Procedures will be reviewed by the benchmark evaluation team and the Bidder will only obtain feedback on the first day of its benchmark. This scheduling and other related details with be discussed further with the Bidder's that successfully reach the benchmark testing stage.
6. If Canada determines during the benchmark test that the Bidder's proposed solution does not meet the mandatory requirements of this solicitation, the Bidder's proposal will be declared non-compliant and be disqualified.
7. Canada may, as a result of any such demonstration, reduce the score of the Bidder on any rated requirement, if the benchmark test indicates that the score provided to the Bidder on the basis of its written proposal is not validated by the benchmark. No Bidder's score will be increased as a result of any demonstration during the benchmark.

8. If a Bidder 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 Bidder (e.g. acts-of-God, war, terrorism or widespread power outages) in which case PWGSC may establish a revised schedule based on the situation.

1.7.1.6 Exclusions

1. There is no requirement to renew/replace the PCS servers or PCS workstations.

1.7.2 ROYAL CANADIAN MOUNTED POLICE (RCMP)

1.7.2.1 Included in Supply

1. GFE servers and AFIS/Transcoder workstations recently procured by RCMP through a GOC National Master Standing Offer (NMSO) and existing Transcoder flatbed scanners. Refer to Annex F which includes all components provided as GFE.
2. Cisco network devices such as Layer three (3) switches and stackable switches. The Layer three (3) switches include the Application Control Engine (ACE) which provides load balancing, Secure Sockets Layer (SSL) termination and synchronous HTTP communication between the RCMP/SSC and the Contractor's VSS solution.
3. Communications Security infrastructure.
4. McAfee ePolicy Orchestrator (ePo) services and McAfee client software as required.
5. Internal/external communications infrastructure.
6. Storage Area Network (SAN) storage.
7. Server room space, hook-ups.
8. RCMP server room racks and server cabling between racks and network switches.
9. Technical support for installation.
10. NPS-NIST Server (NNS) functionality including all interface capabilities based on the ICDs.
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.
12. Coordinating Contractor access to Subject Matter Experts (SMEs).
13. Approval authority for decisions, approvals and sign-off required by Contractor.

1.8 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.
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 could include servers, workstations, printers, scanners, cameras, databases, firmware and any other devices/products required to provide the Entire AFIS renewal solution.

1.9 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.
2. English and French need not appear on a screen at the same time but users shall sign in with either one of the two languages.
3. The Contractor’s Entire AFIS renewal solution shall be functionally equivalent in both official languages (Canadian English and Canadian French) according to Federal Government standards. The Entire AFIS renewal solution must adhere to the following Acts and Policies:
    a. Official Languages document entitled *Official Languages Act* at http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/OffLang/UOLETOC_e.asp; and
    b. The document entitled *Policy on Using the Official Languages on Electronic Networks* at http://laws.justice.gc.ca/en/o-3.01/text.html.
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 ICD.
5. The shortcut keys shall reflect the language of the interface being used (e.g., “N” for “Next” would become “S” for “Suivant”).
6. The software shall use Canadian spelling, either Canadian English or Canadian French (e.g., “colour” instead of “color”).
7. The Entire AFIS renewal solution shall permit users to select their default language of operation as part of their profile.

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.
9. The ICDs in section 1.6 (Compliancy Standards and Reference Documents) contains the code values that are applicable to each input field.
10. The Entire AFIS renewal solution shall make a French and English description available for each code table value.
11. The Entire AFIS renewal solution shall display the description associated with a code table value in the language currently selected by the user.
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 do change.

1.10 SECURITY

1. RTID, AFIS and its subsystems operate in a GOC Protected B environment. The Contractor must be experienced operating and supporting an AFIS in a Protected B environment.
2. The software and document deliverables are consider 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.
3. Any on-site Contractor resources will be assigned an RCMP/SSC Protected A email account. This Protected A email account must be used for all AFIS related email exchanges. Virtually all RTID/AFIS communication is considered Protected A or higher; therefore, Contractor internet email addresses should only be used when the communication is clearly identifiable as non-sensitive.
4. The Security Requirements Check List (SRCL), provided with the RFP, reflects the classification of the data being processed and how documents are to be handled by the Contractor.
5. 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.

6. 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.
7. 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.
8. The physical safeguarding, confidentiality and integrity protection of the RCMP data, systems and applications is of key importance to RCMP. Federal laws and statutes such as, the Government Security Policy, the Access to Information Act, the Privacy Act and the Official Secrets Act, detail specific criteria for the protection of infrastructure and information. The Contractor must support those security requirements in addition to all security requirements described in this SOW. The Contractor must work with the RCMP to ensure these requirements are met.
9. The Contractor shall obtain Personal Security Clearances in accordance with the rules of RCMP's DSB. A Facility Access Clearance is required for all contractors, trades persons, vendors and support personnel prior to scheduling work in the data centre. Managers, supervisors and personnel with computer room access with their building security badge must ensure the necessary steps are taken to comply with this policy. Failure to comply will be considered a breach of security and will be reported accordingly. Individuals with access are prohibited from bringing non-cleared personnel, including family members, into the data centre for tours or any other reason. The Contractor must gain RCMP Top Secret security clearances for a minimum of 2 personnel or the Contractor will be deemed non-compliant and the contract will be terminated. Refer to the Security Requirements Check List (SRCL) included in this SOW for additional details.

1.11 CONSTRAINTS

1. This section identifies the constraints related to this SOW. The Contractor shall review them and confirm acceptance in the proposal submission.
2. The renewed/replaced technology included in the Contractor's proposed solution must be included in the Contractor 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.
3. The Contractor must understand and follow the RCMP Change Management process including the Service Desk change management process, the installation process and release promotion process through various environments to the Production environment. The change management documentation (1.6.3) 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.

4. RCMP will create the Service Desk Change Orders, as required, for activities completed for this SOW. The Contractor must create all the information and documentation required for the Change Records (CRs) and Activity Records (ARs), as documented under this SOW and the RCMP Change Management process.
5. The Contractor is expected to inform the RCMP of anything that could improve the overall solutions requested in this SOW; and/or the efficiency with which the solutions could be implemented. The RCMP has sole responsibility for deciding to use any suggestions presented by the Contractor.
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.
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.
8. Power at the DR site is limited. The replacement AFIS solution must not exceed the power currently used by more than ten (10) percent. Refer to Annex F for the power consumption specifications of the existing servers.

1.12 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 high level MCS, 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.
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.
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.
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 & Schedule.

1.13 WARRANTY

1. Price and rates quoted in the Contractor response must be all inclusive ceiling (or firm) prices, subject to downward adjustment only, and must include but not limited to all labour and replacement parts for a one (1) year warranty period for all non-GFE and GFE modification. This one year warranty period will begin after final acceptance and approval by the RCMP.

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, temporary resident (immigration) and RCMP employee fingerprints. RTID supports submissions from various police agencies, government departments, civil clearance organization and international police agencies to perform criminal record checks. RTID supports extensive latent crime scene print processing for RCMP HeadQuarters' (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.
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).
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.

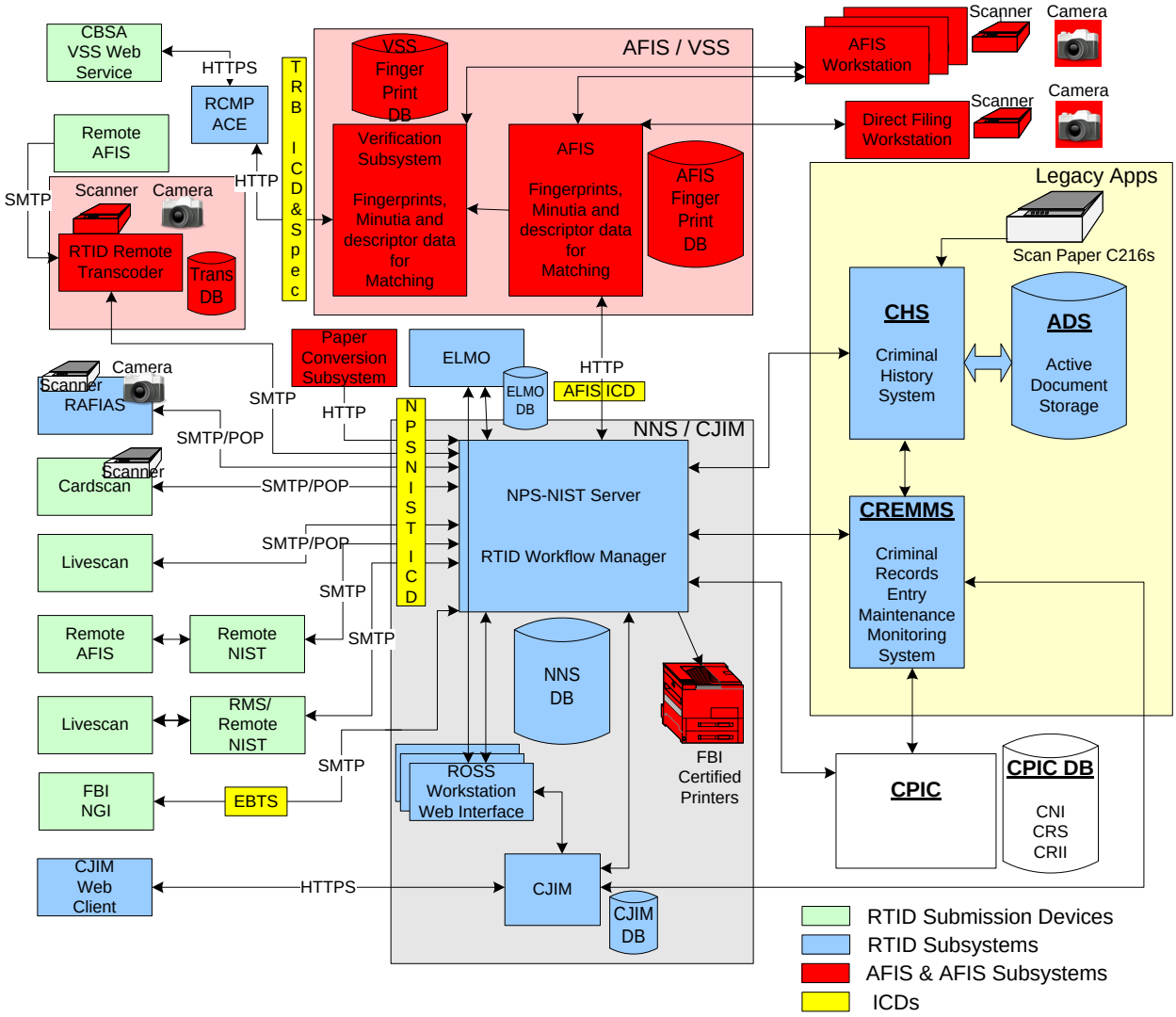

Figure 1: Current High Level RTID Architecture

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

   a. RTID submission devices:

      i. Cardscans, 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 TRB NPS-NIST ICD 2.1.0/2.1.1 for External Contributors. These submission devices could 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 CBSA VSS web service submits to RTID based on the TRB NPS-NIST ICD 2.1.0/2.1.1 for External Contributors and the TRB Verification Interface Specification (refer to 1.6 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 TRB NPS-NIST ICD 2.1.0 for External Contributors. The SSL session is through a secure connection provided by the RCMP/SSC; therefore, there is double encryption;

iii. The Regional Automated Fingerprint Identification Access System (RAFIAS) allows RCMP detachments to submit latent images to RTID based on the NPS-NIST ICD. These latent images are processed on AFIS by latent fingerprint analysts specializing in fingerprint crime scene investigation. Similar to Cardscans, RAFIAS devices can also be used to perform criminal record searches using an individual’s fingerprints and 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 access through a secure portal using the RCMP/SSC ROSS workstation from RCMP premises;

ii. Electronic Maintenance Monitoring Operations (ELMO) is the RCMP Latent case management system which works interactively with NNS to support the RAFIAS Latent submissions. The ELMO UI operates on the RCMP/SSC ROSS workstation with access to the ELMO database on a RCMP/SSC SQL server and includes a few capabilities that are supported through an interface with NNS. The RAFIAS/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 and Active Document Storage maintain criminal record related information processed by or relevant to RTID operations. The Criminal Records Entry Maintenance and Monitoring System (CREMMS) is entry system used to maintain criminal record information maintained on CPIC;

iv. The RCMP/SSC Cisco Application Control Engine (ACE) 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 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 ICD (refer to 1.6 for details);

ii. AFIS workstations interface directly with AFIS to support all AFIS related user activity. AFIS workstations are located at RCMP HQ;

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 ICD (refer to 1.6 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 ICD. The Transcoder must also supports receiving fingerprints/palm prints directly from a remote AFIS to allow larger police agency 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 agency with training 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 Latent 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 Port Of Entry (POE) fingerprints captured when the individual arrives in Canada. This is a 1-to-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 TRB NPS-NIST ICD 2.1.0/2.1.1 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 ACE 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 3 seconds (typically 2.5 seconds) between the RCMP ACE and VSS. This sub-three (3) second response time is measured from the time the ACE sends to VSS and when the ACE receives the complete response from VSS. The VSS renewal must perform as fast or faster than sub-three (3) seconds for any VSS verification request;

    Note: VSS volume and performance details are included in Annex D; however, please note that the Production VSS architecture includes four (4) nodes and the average processing time of the AFIS renewal solution must be less that 0.5 seconds. The current Production VSS, under normal operating conditions, processes twenty-one (21) verification requests in less than ten (10) seconds.

v. The AFIS Paper Conversion Subsystem (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 consider in the response to this SOW;

vi. The AFIS printers used by RTID must be FBI certified printers;

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

viii. Cameras are used by AFIS workstations to scan DCNs/DOCIDs to retrieve and certify a paper submission; and

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

    Note: Separate cameras, not included in the scope of this SOW are used 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.
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.

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 will be presented during the planned vendor conference. 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. The Contractor must also provide training and on-going support for all they key areas.
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.
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.
4. The Contractor's proposed 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. If the AFIS renewal uses different internal ports within the existing security/network architecture, it would be considered an acceptable difference providing it does not create a vulnerability that is unacceptable to RCMP's Departmental Security Branch (DSB). RCMP is solely responsible for determining whether any aspect of the Contractor's proposed solution creates a vulnerability.

5. As part of maintaining RCMP systems, all of the AFIS/Transcoder workstations and many of the AFIS servers have recently been replaced using Government Of Canada (GOC) National Master Standing Offers (NMSOs). These workstations and servers are considered GFE for this AFIS renewal SOW and they are listed in Annex F. The GFE AFIS/Transcoder workstations use the Windows 7 Operating System (OS) and the Contractor's proposed User Interface (UI) for the AFIS/Transcoder fingerprint analyst must operate on these workstations with Windows 7 or Windows 10 desktop OS. Although not mandatory to utilize the GFE servers, they are available to implement the Contractor's solution. 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.
6. 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 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.
7. 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 PCS in being decommissioned; therefore, it does not have to be considered in this SOW. 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.

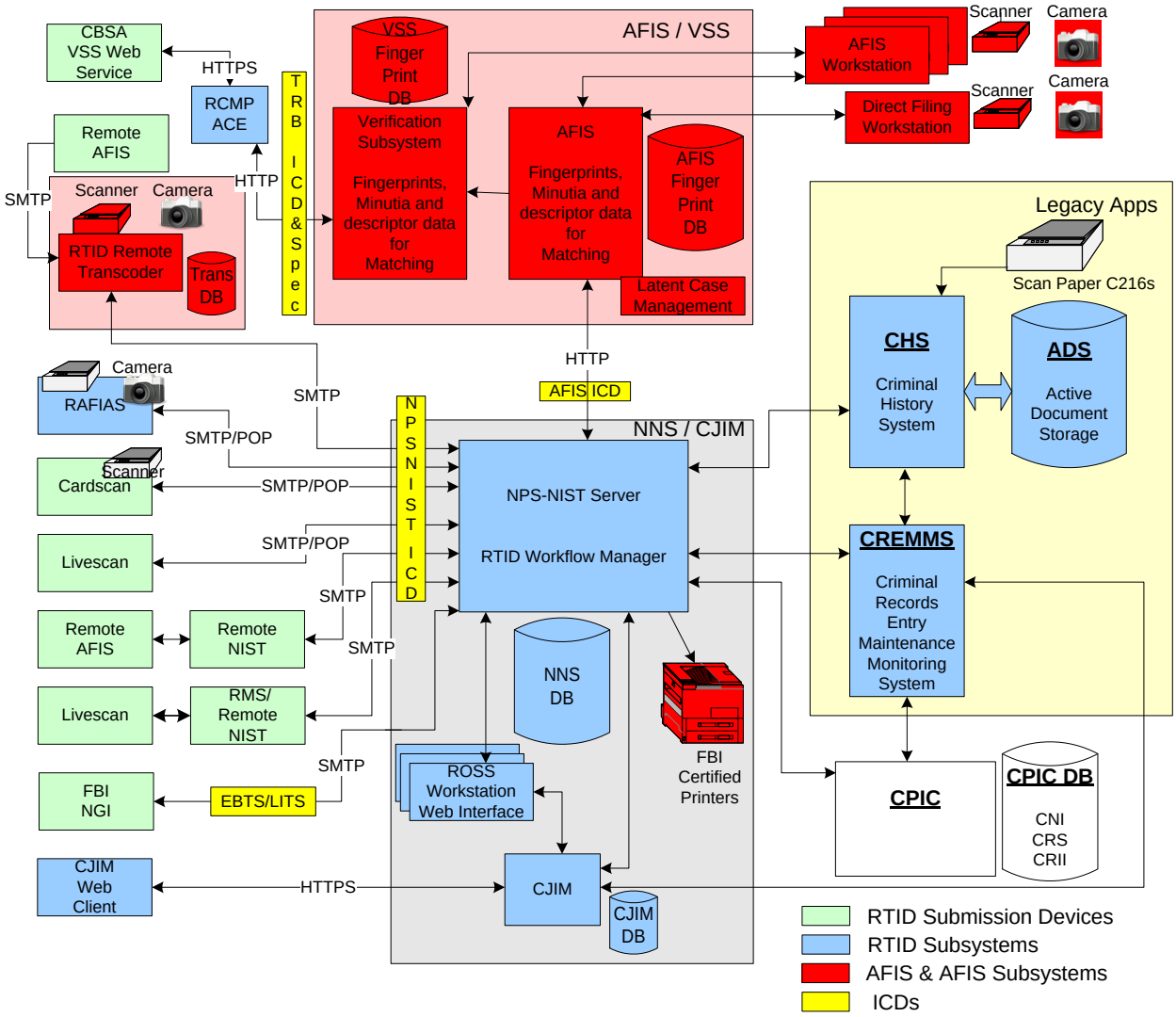

Figure 2: Entire AFIS Renewal High Level RTID Architecture

3.2.1 AFIS PRODUCTION AND THREE TEST ENVIRONMENT RENEWAL

1. The AFIS renewal must include the following:
   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 a sync filing capability, during the transition, where the Contractor's AFIS must support receiving electronic transactions from NNS and processing them completely without responding back to NNS. This will allow the two 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 processing legacy transactions 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 a dual Data Center configuration that allows fail-over from RCMP's Primary (PR) site to the Disaster Recovery (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 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.

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.

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).

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.

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 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; and

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.

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

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.
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 analysts that uses an AFIS workstation.
3. The Transcoder must interface with RTID using the NPS-NIST ICD and communicate with RTID through bi-directional SMTP over a secure communication link.
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.
5. The Transcoders must provide:
    a. The required functionality as stated in this SOW and its annexes;
    b. A scanner for scanning Latents; and
    c. Allow latents captured using 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.
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).
8. The Transcoder must support bi-directional SMTP between the Transcoder and RTID;
9. The Contractor's solution must include the database conversion from the existing Transcoder database to the Contractor's Transcoder database;
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; and
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.

3.2.3 VERIFICATION 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 Temporary Resident's fingerprints received from a CBSA POE to validate an individual's identity.
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.
3. The Contractor's solution must include the database conversion from the existing VSS database to the Contractor's VSS database.
4. The VSS must be able to operate independently from the AFIS.
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.
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 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;
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;
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);
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; and
10. All production and test environment servers must be maintained with the latest updates for the existing 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 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.

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.
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. 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.
3. The Contractor's solution must include the database conversion from the existing ELMO SQL database to the Contractor's LCMC database.
4. The LCMC must comply with the Scientific Working Group on Friction ridge Analysis, Study and Technology (SWGFAST) Analysis, Comparison, Evaluation and Verification (ACE-V) methodology.
5. The Contractor must demonstrate the LCMC/AFIS ability to support SWGFAST ACE-V through the LCMC/AFIS processing and documentation generated as part of the processing.
6. 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.

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:
    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.

3.2.6 ONGOING SUPPORT

1. The Contractor must provide at least one (1) permanent on-site resource at RCMP HQ in Ottawa, Canada.
2. This resource must be available on-site during RCMP core hours (8am-5pm eastern time).
3. The Contractor on-site resource must:
    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, 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.;
    e. One (1) hour response time for production or test environment issues during on-site hours;
    f. 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 (GoC) 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, 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 abel to respond to question, resolve problem, 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.

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.
2. This FRC does not need to be implemented with the scope of the initial procurement of the AFIS renewal. The FRC is considered a future requirement that will be implemented after the mandatory requirements in the AFIS renewal solution have been implemented.
3. Section 12 describes the detailed FRC requirements that should be satisfied by the Contractor at the time of the Contractor bid submission.

3.2.8 CONVERSION

1. The Contractor must convert of all data used by AFIS and its subsystems to a format that is usable by the Contractor's proposed solution.
2. The conversion must be completed on RCMP premises within the RCMP/SSC security architecture.
3. The Contractor must provide a high level plan and strategy with its proposal explaining:
    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.

4. OVERVIEW OF RENEWAL APPROACH

4.1 PURPOSE

1. This section provides an overview of the approach that RCMP expects with the Entire AFIS renewal solution. It 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 that will be renewed.

4.2 OVERALL APPROACH

1. There are currently three test environments DEVTEST, QCS and MAINT and the production environment. 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.
2. A separate RTID test environment will be established for the AFIS renewal solution which will be referred to herein as the AFIS-Renew environment. This AFIS-Renew environment will be used by the Contractor in the same manner that the MAINT environment is typically used. That is, the MAINT environment is typically the environment used by the Contractor 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.
3. This AFIS-Renew environment must be used by the Contractor to verify that all aspects of the AFIS renewal solution satisfy all functional, technical, interface and processing requirements for a test environment including support for the interface specifications and ICDs. The Site Acceptance Test Plan (SATP) and Site Acceptance Test Report (SATR) 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.
4. 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 in the AFIS-Renew environment. This site acceptance testing by the RCMP will include testing all RTID functionality by the RTID test team.
5. After RCMP approval of AFIS renewal solution in the AFIS-Renew environment, the AFIS renewal solution will follow the RTID release process or the RCMP agreed to adjustment to the release process in the Contractor’s ARIP.
6. To ensure maximum flexibility for the Contractor to use the GFE, system testing and QCS testing can be completed in the Contractor’s parallel production environment configuration. This allows the DEVTEST and QCS environments to remain as is until after final acceptance. The Contractor can use GFE from the test environments to configure the parallel production environment as long as the RCMP has an environment to support existing production until the cut-over to the AFIS/Transcoder/VSS renewal solution has been completed. Additionally, the Contractor can configure an initial production environment that partially supports the full production requirements, with at least fifty percent (50%) production capacity for 2019 volumes, and then reuse existing production servers after the cut-over to achieve one hundred percent (100%) capacity .

7. The AFIS Renewal Implementation Plan (ARIP) (DID AR-01) 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.
8. 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.
9. 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.

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.
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 the MCS.
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.
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.
5. Workstation upgrades must be fully tested and approved before Production workstations can be upgraded. Existing workstations will be allocated for the AFIS-Renew environment and the parallel AFIS renewal production environment.
6. The QCS environment must be used to test all the HA capabilities of the Contractor's AFIS renewal solution. The RCMP will lead all testing in the QCS environment. 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 testable in the QCS environment unless agreed to in writing by the RCMP.
7. 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.

8. The Production AFIS renewal solution 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 AFIS renewal solution fully supports all the requirements in this SOW and its accompanying documents, the existing AFIS will be disabled and the AFIS/Transcoder/VSS renewal solution will become the system of record for AFIS processing. These release activities to make the AFIS/Transcoder/VSS renewal solution operational in the Production environment will be completed during a weekend RTID outage. The precise length of the weekend 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.

4.4 RCMP ACCEPTANCE

1. RCMP acceptance testing will only start after the Contractor has successfully demonstrated that the replaced/upgraded/reuse components are fully operational. The SATR must be completed to document the successfully demonstrated component(s) operation.
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.
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.
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 or, based on prior approval by the RCMP, tested in the Production environment. This SOW and its accompanying documents identify the minimum HA testing that must be testable in the QCS environment. It is preferred that all HA capabilities are testable in the QCS environment.
5. The full scope of the existing testing that is used by the RCMP is available for the Contractor's review as required.

4.5 IMPLEMENTATION STAGES

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

2. To ensure it is clear, these two stages include installation, implementation, integration, conversion, interoperability and set-to-work activities required for all environments, following the RCMP/CIO release process or the RCMP agreed to process in the ARIP.
3. All the training required with this initial procurement will be completed in stage one (1) or stage two (2).
4. It is preferred that the implementation to support EFS is completed as soon as possible after stage two (2); 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 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. This strategy must be included with the Contractor's proposal which will be consider part of the evaluation assessing support for EFS.
5. Facial recognition will 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.

5. CONTRACTOR CORPORATE AND MANAGEMENT REQUIREMENTS

5.1 PURPOSE

1. This section describes the high level corporate and management requirements that must be satisfied by the Contractor. Annex I describes the detailed requirements that must be satisfied by the Contractor.

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.

5.2.2 SUBCONTRACTOR MANAGEMENT

1. For those elements of the required work defined in this SOW, its annexes/appendices and compliancy documents that are provided to Subcontractors, the Contractor shall ensure that all relevant work and contract terms, conditions and requirements are accepted and understood by the Subcontractors. The Contractor shall maintain full responsibility for all work assigned as a part of the contract resulting from this RFP.
2. The Contractor shall ensure that any subcontracting arrangement is approved by the RCMP and that management of subcontractors is transparent to the RCMP Project Authority (PA).
3. The Contractor will be responsible for all work, activities and actions of the subcontractor and must ensure that any applicable requirements of the Contract resulting from this SOW are promulgated to all subcontractors.

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:
    a. The proposed resources and their qualifications;
    b. The roles and responsibilities of each resource;
    c. The reporting relationship, including the resources reporting relationship to their senior management; and
    d. 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.

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 ROCs and reporting request, and perform the tasks associated with SOW and its accompanying documents.
2. The Contractor's SPOC and any other proposed resources directly interacting with the RCMP must have good oral and written communication skills;

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.

5.4 SECURITY MEASURES

1. Security procedures shall be applied by the Contractor for the protection of sensitive information that may be viewed or processed by the activities of this SOW. The security procedures shall comply with the SRCL and this SOW.
2. The Contractor shall ensure that personnel involved with control or access to sensitive information that is to be provided, processed or developed during the activities related to the Contract resulting from this SOW have the requisite security clearance.
3. Visits to the RCMP sites by the Contractor shall be requested through the PA after the visit clearance request "DMAS-DSS 1810" has been approved. Each visit request must:
    a. be provided with a minimum of ten (10) working days lead time for approval; and
    b. identify the purpose of the visit, contractor personnel involved, and security clearance for each such individual.

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 accompany documents. The detailed requirements that must be satisfied by the Contractor's AFIS renewal solution are described in Annex B.

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.
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.

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 environment 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.

6.3.2 FUNCTIONALITY

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

6.3.3 LOAD BALANCING SCALABILITY WITH CISCO ACE

1. For security, performance, scalability and load balancing reasons, the RCMP has implemented OSI layers 4-7 content switching with load balancing and Network Address Translation (NAT) support through Cisco network devices configured with ACE 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 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
2. The Contractor's AFIS renewal solution must support the ability to use the RCMP's Cisco ACE technology to enable load balancing to multiple Contractor servers providing intra-site and inter-site HA.
3. The AFIS servers must be able to send responses to VIPs defined on the ACE destined to RCMP servers.
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.
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 unless agreed to in writing by the RCMP.
6. The specific load balancing techniques required by the Contractor's AFIS renewal solution must be explained in the Contractor's proposal.
7. Any details concerning the RCMP ACE can be provided by the RCMP upon request; however, ACE related information is available online.
8. Refer to Annex A for a more detailed description of the requirements each AFIS environment must support.

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.

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.

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. Refer to Annex A for a more detailed description of the requirements each AFIS environment must be able to support.

6.3.7 SNMP REPORTING

1. The Contractor's servers in all environments must support SNMP reporting to RCMP's Spectrum/eHealth 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.
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.

6.3.8 MCAFEE ANTI VIRUS (AV) SCANNING

1. The Contractor's servers in all environments must include McAfee AV scanning, preferably participating in RCMP's ePo; however, as a minimum 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.
2. 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 determine timeframe. The Contractor's solution must be able to support the automatic RCMP ePo updates.
3. 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 workstation to eliminate the potential impact of the new policies affecting AFIS workstation operations. The policies defined in these containers for AFIS workstations must be determine through the normal release process, testing AFIS in each test environment, prior to release in the Production environment.

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 3 weeks of receiving the update; however, these timing can changed based on RCMP policy decisions.
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. The Contractor's AFIS workstation solution must support receiving and automatically processing WSUS updates.

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.

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.
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.
3. The RCMP ACE 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 ACE load balancing to a single server.
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.

6.3.12 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.

6.4 COMMON TEST ENVIRONMENT REQUIREMENTS

6.4.1 GENERAL

1. This section describes the high level functional and technical requirements that the Contractor must support for all test environments.
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 difference 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.
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.

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.
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 5 different NNS environments.

6.5 SPECIFIC TEST ENVIRONMENT REQUIREMENTS

6.5.1 AFIS DEVTEST

6.5.1.1 General

1. This section describes the technical requirements that the Contractor must support for the DEVTEST environment.

6.5.1.2 AFIS DEVTEST Performance Requirements

1. The current DEVTEST environment database size is:
   a. 5000 Ten Print records;
   b. 1534 Finger latents; and
   c. 204 Palm latents.
2. Based on a growth of 5% per year, the DEVTEST environment must meet or exceed the following performance measurement requirements for the next five (5) years:

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 AFIS DEVTEST AFIS;

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.

6.5.2 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.

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. Refer to Annex A for a more detailed description of the requirements each AFIS environment must be able to support.

6.6 PRODUCTION ENVIRONMENT REQUIREMENTS

6.6.1 GENERAL

1. This section describes the high level functional and technical requirements that the Contractor must support for the PROD environment.
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 accompany documents.

6.6.2 CAPACITY AND PERFORMANCE REQUIREMENTS

1. The Contractor must ensure all capacity and performance requirements stated in this SOW and its accompany 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.
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. Only a minimal number of components can be considered passive standby components in case of a failure.
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.

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 accompany documents.
2. The Contractor's AFIS renewal solution must support all the DR requirements stated in this SOW and its accompany documents. The PROD environment is the only environment with DR site requirements.
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.

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.

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 accompany documents. The detailed requirements that must be satisfied by the Contractor's Transcoder renewal are described in Annex C.

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.
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.

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 difference 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.

7.3.2 FUNCTIONALITY

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

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 determine timeframe. The Contractor's solution must be able to support the automatic RCMP ePo updates.

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 determine through the normal release process testing Transcoders in each test environment prior to release in the Production environment.

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.

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.

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 accompany documents. The detailed requirements that must be satisfied by the Contractor's VSS renewal solution are described in Annex D.

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.
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.

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 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.
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 difference 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.

8.3.2 FUNCTIONALITY

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

8.3.3 LOAD BALANCING SCALABILITY WITH CISCO ACE

1. The Contractor's VSS renewal solution must support the ability to use the RCMP's Cisco ACE technology to enable load balancing to multiple Contractor servers providing intra-site and inter-site HA.
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.
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.
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.
5. Any details concerning the RCMP ACE can be provided by the RCMP upon request.
6. Refer to Annex A for a more detailed description of the current AFIS architecture that must be supported.

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.

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. 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.

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.

8.3.7 SNMP REPORTING

1. The Contractor's VSS servers in all environments must support SNMP reporting to RCMP's Spectrum/eHealth 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.

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.

8.3.8 MCAFEE ANTI VIRUS (AV) SCANNING

1. The Contractor's servers in all environments must include McAfee AV scanning, preferably participating in RCMP's ePo; however, as a minimum 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.

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 3 weeks of receiving the update; however, these timing can changed based on RCMP policy decisions.

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.

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

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.

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.
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.
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.

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.

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.

8.6 PRODUCTION ENVIRONMENT REQUIREMENTS

8.6.1 GENERAL

1. This section describes the high level functional and technical requirements that the Contractor must support for the PROD environment.

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 accompany documents.

8.6.2 CAPACITY AND PERFORMANCE REQUIREMENTS

1. The Contractor must ensure all capacity and performance requirements stated in this SOW and its accompany 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.
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.
3. If the PR site fails, the VSS renewal solution must support at least fifty percent (50%) of the VSS capacity and performance requirements.

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

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.

9. LATENT CASE MANAGEMENT CAPABILITY

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.
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 fingerprints/palm prints for search from the LCMC and perform all other required capabilities stated in this SOW and its accompanying documents.
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.
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 LCMC and AFIS. That is, this integrated LCMC capability would be part of the AFIS renewal solution UI, where additional button or UI icons on the AFIS renewal solution UI would be clicked by the user to perform case management activities.
5. ELMO currently records in its database a significant portion of data that is also recorded in AFIS. The LCMC is expected to eliminate all of this duplication. 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.
6. The Contractor's solution must include the database conversion from the existing ELMO SQL database to the Contractor's LCMC/AFIS database.

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

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.

   Note: Transcoders procured directly by other Police agencies are not included in this SOW. They are expected to have a separate support contract.

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 this SOW have been replaced, upgraded or reused.

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.
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, 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.
3. All the Contractor 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.

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.

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 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.
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.
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.
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 financial proposal provided by the Contractor.

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.

12. FACIAL RECOGNITION CAPABILITY (FRC)

12.1 GENERAL

1. This section describes the functional and technical requirements for the Facial Recognition Capability (FRC) solution.
2. The Contractor must support a 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.
3. 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.

12.2 FRC REQUIREMENTS

1. The suspect photos will typically be from surveillance videos, Closed-Circuit Television (CCTV), handheld cameras including cell phones, or other non-controlled, poor-quality sources. In many cases, only partial facial images will be showing. The FRC will be required to perform a one to one (1:1), and a one to many (1:N) digital facial comparisons.
2. Prior to implementation, the FRC must support the following requirements:
    a. Perform searches involving a known or unknown single photo to a target ID photo looking to confirm identity or suspected identity (one to one match);
    b. Search the photo database using a known photo to discover if the person is in the AFIS/FRC database under other aliases (one to many search);
    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 to many search) 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 to many search) 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 Facial Recognition solution (FRS) shall be capable of saving then as JPEG 2000.

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

5. Prior to implementation, the Contractors FRC must have been measured against the NIST Face Recognition Vendor Test benchmark.

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.
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.
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 may be controlled from Ottawa through a secure remote connection to the Transcoder site in order to complete the data conversion.
4. The data conversion must include an audit trail of all conversion activity, which must include recording when any error occur or when any data mapping occurs where the data is represented differently in the Contractor's solution than in the original data set.
5. The existing RCMP AFIS database, TRB database, VSS database and Transcoder databases will be exported to ANSI NIST compliant formatted electronic files and include FBI EBTS compliant Type-9 minutia records. The Contractor must complete the data conversion for AFIS, TRB, VSS and the Transcoders using the following data.:
    a. The TP/PP NIST files may 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 LT/PL NIST files will include the following NIST records:
        i. Type-1 – Header,
        ii. Type-2 – Demographics,

iii. Type-9 – Minutiae Record (FBI EBTS Complaint) (Existing Latent minutia, plotted by RCMP, is expected to be retained for LT data. If not, the Contractor must explain the impact of retaining the existing AFIS LT minutia on the Contractor's solution), 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 solution.

6. The log files for AFIS, TRB, 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. It is preferable that the converted log files could be used by the Contractor's solution; however, as log as the log data remains unaltered and is searchable by the alphanumeric data to allow individual log record to be identified, it would be an acceptable solution.
7. The ELMO data to be converted is describes in detail in Annex E. The ELMO log files do not need to be converted, since the AFIS log file will be used to identify the historical activity against the case file data in ELMO.
8. The AFIS and Transcoder user management database conversions must also adhere to the requirements herein and be described in the Data Conversion Plan.
9. 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.

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.
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.
3. The Contractor shall:
   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.

5. The Contractor shall prepare and document test cases, including expected results, for each conversion requirement.
6. The Contractor shall carry out testing of the conversion software prior to Site Acceptance Testing.
7. The Contractor, under the supervision of the RCMP, shall perform Site Acceptance Testing of data conversion software, utility(ies) and processes.
8. The Contractor shall provide conversion statistics, including total number of records to be converted, total number successfully converted, problems encountered and their resolution.
9. The Contractor shall provide controls to ensure that data converted maintains its integrity and referential integrity throughout all processing routines.

13.3 DATA CONVERSION DETAILS

1. Data conversion refers to those activities and deliverables necessary to migrate existing AFIS data from the current AFIS to the AFIS renewal solution.
2. 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.
3. The Contractor shall ensure that the single Subject Identification Number can include multiple sets of images and fingerprint characteristics.
4. The Contractor shall ensure that the single Subject Identification Number includes up to six (6) file numbers, with four currently implemented. Refer to the AFIS ICD for details.
5. The Contractor shall be responsible for loading all reference tables required for the AFIS solution.
6. The Contractor shall be responsible for populating all administrator tables and configuration parameters.
7. 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.
8. The Contractor shall carry out the Data Conversion process as per the approved Data Conversion Plan.
9. 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 fomat, 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).
10. The data volumes are included in Annex B, AFIS detailed requirements.

13.3.1 DATABASE CONVERSION NUANCES

1. The following identify nuances that must be used by the Contractor in the database conversion process, as well as in normal day-to-day processing.

a. For consolidations, in conversion and through normal processing, involving 2 or more Refugee records the following ordinal numbering scheme is to be used from lowest to highest:
   i. 330008xxxx, and
   ii. 330001xxxx,
   iii. Thus, the 330008 is always the lowest, the oldest, of the numbering sequence and then the numbering sequence would follow the “normal” ordinal numbering.

2. For consolidations and normal processing, the following ordinal numbering scheme must be used where appropriate to support the requirements stated through this SOW and its accompanying documents
   a. The short format of an FPS Number is either a 1 to 6 digit numeric or a 1 to 6 digit numeric + a letter. 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 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,
      x. No letter (non alpha) = 9,
   b. When printing Non Alpha file numbers as part of the barcode, the ‘9’ must be replaced by a blank (i.e. space character).

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.

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 different subjects or file numbers).
3. The Contractor shall ensure that the Project Authority is provided with at least two (2) weeks to review and approve the process for carrying out the clean up of these multiple filings.
4. The Contractor shall ensure that a process is defined and implemented to carry out the clean up where duplicates and other discrepancies are found.

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.
2. The Contractor shall enable the RCMP to verify these highly probable hits.
3. The Contractor shall ensure that the RCMP Project Authority is provided with at least two (2) weeks to review and approve the process for carrying out the clean up of these latent hits.
4. The Contractor shall ensure that a process is defined and implemented to carry out the clean up where latent hit to ten print and discrepancies are found.
5. ULF entries with the same minutia for the same case should not be converted.
6. The Contractor shall identify ULF entries that belong to the same case/image (same minutiae).
7. Duplicate ULF entries that belong to different images (meaning different minutiae) even if they belong to the same case should not be consolidated.
8. ULF entries belonging to different cases should not be consolidated.
9. The Contractor shall enable the RCMP Latent technician to verify/approve the consolidation of ULF entries.
10. 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.

13.6 DATA CONVERSION APPROACH

1. The Contractor will follow the data conversion guidelines outlined in this section.
2. The RCMP will provide:
    a. A small amount of Government-provided space in the RCMP HQ complex in Ottawa or alternate Ontario conversion site 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.
4. The Contractor shall provide all of the equipment and personnel to conduct the necessary conversion operations.
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.
6. Conversion Records
   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:
   a. 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);
   k. Previous DCN (if applicable);
2. The Contractor shall back up the complete file at least once a day.

3. The Contractor shall maintain an up-to-date backup copy of the complete file.
4. The Contractor shall maintain the Conversion Audit Trail for the life of the AFIS contract.
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) days of the end of the last AFIS conversion activity.
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 may be submitted unless supported by a valid rationale (e.g., directed rescan). RCMP approval is required for all subsequent submissions.
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.

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.
2. The Contractor shall integrate and test its production system with the converted date in accordance with its approved SATP.
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.
4. The Contractor is 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.

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.
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 document.
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:

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 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 all the documentation required to support the claims in their proposal. The documentation provided will be used to determine if the Contractor's proposal is compliant; therefore, comprehensive documentation including architecture diagrams, design documents, preliminary ARIP with 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.
2. The premilinary 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.
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.

15. OVERALL DELIVERABLES PLAN & SCHEDULE

15.1 OVERVIEW

This section identifies the Contractor major deliverables and describes the content of the deliverables that must be completed as part of this SOW. 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.

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. 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).

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 Contractor's financial proposal. The table in Annex D may 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.

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. 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 Project Technical Authority.

15.2 CONTRACT DELIVERABLES REQUIREMENTS LIST (CDRL) SCHEDULING OF DELIVERABLES

The following table identifies the deliverables, responsibility for completion, initial delivery date, revision time period and final deliverable dates. The time estimates are preferred by the RCMP. 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.

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 Contractor's financial proposal.

Note: The Implementation Steps and information required for the RFC/AR process will be according to the Chief Information Office (CIO) Sector's Change Management policy as referenced in the Maintainability subsection of this SOW.

Note: All dates in the tables below are calendar dates. The *RCMP Review* column represents business days.

Table 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 before Contract Award (CA)	5 days	After Contractor review and agreement	10 days after review and agreement
2.	Project 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)	AT-01	the Contractor	With proposal, for RCMP use, to validate compliance to AFIS Renewal RFP requirements	TBD	For use with ATP/SATP to verify implementation satisfies all requirements	As depicted in PM-01 Gantt Chart
5.	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
All other deliverables							
1.	Delivery of Bill Of Materials (BOM)	N/A	the Contractor	TBD	N/A	N/A	As depicted in PM-01 Gantt Chart
2.	Delivery of hardware	N/A	the Contractor	As depicted in PM-01	5 days	N/A	As depicted in PM-01 Gantt Chart
3.	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

No	Description	DID No	Responsible	Initial Delivery Date	RCMP Review	Updated	Final Delivery Date
4.	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
5.	Implementation Steps & information required for RFC/AR Process	CM Process[2]	the Contractor	As depicted in PM-01	5 days	After RCMP Review	As depicted in PM-01 Gantt Chart
6.	RFC / AR Creation	CM Process	RCMP	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
7.	Acceptance Testing (Functional)	Using RCMP Test Plans	RCMP	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
8.	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
9.	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
10.	Ongoing OS & Software Upgrade	OU-01	the Contractor	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
11.	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
12.	Software and Documentation	DO-01	the Contractor	N/A	5 days	After RCMP Review, and after completion of Acceptance Testing	As depicted in PM-01 Gantt Chart

[2] Change Management Process – Refer to Maintainability subsection

No	Description	DID No	Responsible	Initial Delivery Date	RCMP Review	Updated	Final Delivery Date
13.	Milestone Payments	N/A	the Contractor/ RCMP	As depicted in PM-01	N/A	N/A	As depicted in PM-01 Gantt Chart
14.	Final Acceptance	Review DO-01	RCMP	N/A	N/A	N/A	As depicted in PM-01 Gantt Chart
15.	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	2. IDENTIFICATION NUMBER
Master Contract Schedule (MCS)	PM-01

3. DESCRIPTION/PURPOSE

The Master Contract Schedule (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 Project 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 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	2. IDENTIFICATION NUMBER
Progress Review Meetings (PRM)	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 Project and Technical Authorities;

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;

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 special meetings. Special 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 project 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 AFIS Renewal Implementation Plan (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 financial proposal provided by the Contractor, 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 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 an 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 backout 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;
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,
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.

Host name & 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			
		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	2. IDENTIFICATION NUMBER
Acceptance Testing - Acceptance Test Plan (ATP)	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 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 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 throughouit 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. A Requirements Traceability Matrix (RTM) shall be provided which describes or demonstrates how the Contrator'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	2. IDENTIFICATION NUMBER
Acceptance Testing - Acceptance Test Report (ATR)	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 TA 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 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

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 Project Authority and Technical Authority have 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

5. TITLE	6. IDENTIFICATION NUMBER
Acceptance Testing - Site Acceptance Test Plan (SATP)	AT-03

7. 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.

8. PREPARATION INSTRUCTIONS

8.1 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.

8.2 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.

8.3 Content Requirements. As a minimum, the SATP 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 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;

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 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:

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

viii. A Requirements Traceability Matrix (RTM) shall be provided which describes or demonstrates how the Contrator's Proposed Solution satisfies all the requirementsidentified in this SOW and its accompanying documents for the scope of SATP;

ix. 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;

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

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

xii. 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;

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	2. IDENTIFICATION NUMBER
Acceptance Testing - Site Acceptance Test Report (SATR)	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 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:

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. Evaluation and Recommendations. This section shall be divided into the following paragraphs:

i. Evaluation. 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 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 Project Authority and Technical Authority have 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 that the Contractor deems relevant to enhance the document and that is not addressed elsewhere in the DID; and

j. Attachments. 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 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 high level design for the Proposed Solution which results from the Contractor's review and analysis of the Proposed Solution Requirements and Specifications stated in the SOR 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 SOR. 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:

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

j. 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 SOR and its appendices;

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

l. 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;

m. 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.;

n. 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.);

o. 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:

x. 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.;

xi. 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;

xii. 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;

xiii. 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

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

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

j. 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;

k. 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;

l. 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;

m. 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;

n. Security Plan. This section shall detail the security architecture of the 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;

o. 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;

p. 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;

q. 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;

r. 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:

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 (eg. replication and synchronisation of directories, etc.) along with expected time required for such activities;

y. 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.);

z. 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;

aa. 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.;

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

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

dd. 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 UPGRADE (OOSU)

DATA ITEM DESCRIPTION

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

Note1: 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).
Note2: 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.;

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:

xv. Host name;
xvi. IP address (not included herein for security reasons);
xvii. Function;
xviii. Model;
xix. CPU;
xx. Memory;
xxi. Disk storage available;
xxii. Operating System including version and service pack / patch number;
xxiii. End-of-life date;
xxiv. End-of-service date;
xxv. Hosted software;
xxvi. An indication if SAN is required for the component and if so how much is allocated;
xxvii. Date of the last upgrade;

xxviii. 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;
xxix. Issues, concerns and/or notes associated with the upgrade; and
xxx. 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.

Host name	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					
		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	2. IDENTIFICATION NUMBER
Software and Documentation	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 annex is to define the terminology used within this Statement of Work.

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 SLA, retention period for files, 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 Temporary Resident (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.
Fingerprint Biometric Data	This term refers to fingerprint images contained within a Submission.
IID Number (Immigration Identification Number)	The Immigration Identification File Number is the unique key generated by the RCMP under which Temporary Resident data is stored within the RCMP. • An IID Number, once purged, will never be reused.

Term	Definition

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 TRB project include:
	  • Internal ICDs (e.g., AFIS ICD and IIS ICD);
	  • External ICDs (e.g., NPS-NIST ICD 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 TR Subject File and TR 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 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 TPREI.
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
Submission	A request for service initiated by an external contributor to add, retrieve, amend, remove or search for information held in the Royal Canadian Mounted Police (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 ERRT; • an ACKT; and • an SRE.

Term	Definition
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.
Subject	An identifies 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 Sibject Id.
Submission	This term refers to an RTID request, primarily based on the NPS-NIST external ICD; however, there are some internal request that result in submissions. Submissions generally result in multiple transactions being processed to execute a specific workflow. Refer to the ICD for specific details.
Submission Data	This term refers to the 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…
TR Verification Repository	This term refers to the Temporary Resident biometric fingerprint and encoding (minutiae) created and retained for Verification purposes. It also includes the image data and biographical information.
Transaction	This terms refers to a defined interaction within a submission. An exchange of information with the system or a sub system.
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 Fingers • Left Four Fingers • Two 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.
Verification	Comparing a candidate fingerprint/palm print to a search fingerprint/palm print.
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 a TR enrolment may be kept for 30 days after completion of service prior to data clean-up.

Term	Definition
Work in Progress (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

Table C-1: List of Acronyms

Acronym	Definition
ACKT	Acknowledgement Transaction
AFIS	Automated Fingerprint Identification System
ANSI	American National Standards Institute
ATP	Acceptance Test Plan
ATR	Acceptance Test Report
BSO	Border Services Officer
CBSA	Canada Border Services Agency
CCRTIS	Canadian Criminal Real Time Identification Services
CDRL	Contract Deliverables Requirement List
CIC	Citizenship and Immigration Canada
CIO	Chief Information Officer
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf System
CPIC	Canadian Police Information Center
CSR	Contractor Status Report
DID	Deliverable Item Description
DCN	Document Control Number
EFCD	Electronic Fingerprint Capture Device
ERRIN	Internal Error Transaction
ERRT	Error Transaction
ERRV	Error on Verification Transaction
FBI	Federal Bureau of Investigation
ICD	Interface Control Document
IID	Immigration File Number
ILRI	Image List Retrieval
IMA	Temporary Resident Amend Transaction
IMAR	Temporary Resident Amend Response
IMM	Temporary Resident Enrolment Transaction
IMP	Temporary Resident Purge Transaction

Table C-1: List of Acronyms

Acronym	Definition
IMPR	Temporary Resident Purge Response
IRQ	Fingerprint Image Request
IRR	Image Request Response
MCS	Master Contract Schedule
NNS ICD	NPS-NIST External ICD
NPS	National Police Service
NIST	National Institute of Standards and Technology
ORI	Originator
POE	Port of Entry
PRM	Progress Review Meetings
RCMP	Royal Canadian Mounted Police
RTID	Real Time Identification (system)
SDD	System Design Documentation
SIP	Site Installation Plan
SATP	Site Acceptance Test Plan
SATR	Site Acceptance Test Report
SLA	Service Level Agreement
SOW	Statement of Work
SRE	Search Response
SRV	Verification Search Response
STI	Status Transaction
TBD	To Be Determined
TCN	Transaction Control Number
TPAI	Ten Print Amend
TPCNI	Ten Print Consolidation transaction
TPCNRI	Ten Print Consolidation Response
TPDI	Ten-Print Delete Request
TPQCI	Ten Print Quality Control Response
TPREI	Ten Print Request Response
TPRI	Ten Print Search Request

Table C-1: List of Acronyms

Acronym	Definition
TR	Temporary Resident
TRB	Temporary Resident Biometrics
UI	User Interface
VER	Temporary Resident Verification Transaction
WI	Work Item - RCMP Software/Solution Incident Report
WIP	Work in Progress