Systems Delivery and Project Portfolio Management (SDPPM)

Electronic Fingerprint Capture Devices (EFCDs)
National Master Standing Offer
Request For Standing Offer (RFSO)

APPENDIX A:
EFCD STATEMENT OF REQUIREMENT

Last Updated Date: 2020-06-30

Status: Final

Version: 1.3

RDIMS Document No.: 45326v3C

TABLE OF CONTENTS

TABLES

FIGURES

1. INTRODUCTION

1.1 General

1. In order to support ongoing operational requirements for Real Time Identification (RTID), the Royal Canadian Mounted Police (RCMP) requires the establishment of a National Master Standing Offer (NMSO) for Electronic Fingerprint Capture Devices (EFCDs). The purpose of this NMSO is to provide a contracting mechanism for the RCMP, the Government of Canada (GC) (including Departmental Corporation or Agency, or other body of the Government of Canada) as well as all Canadian Provincial/Municipal Governments (CPMGs) to procure EFCDs in support of operational requirements to submit electronic biometric (e.g., fingerprint, palm print, photo) and biographical data (e.g., name, date of birth) to RCMP's RTID System. (I)
2. This Statement Of Requirement (SOR), its accompanying annexes and compliancy documents describe the requirements that must be satisfied to replace the existing EFCD NMSO. These requirements include both Livescan and Cardscan EFCDs; and Simple Mail Transfer Protocol (SMTP) Single Point Of Interface (SPOI) Servers when there is more than one EFCD at an agency. (M)
3. This NMSO will be considered a contracting mechanism to supply a turnkey solution for the devices included in this NMSO Request For Standing Offer (RFSO). There will be no planned design reviews or other similar project type activities that will be part of the NMSO contract. Instead, an evaluation will be performed on the Livescan/Cardscan NMSO bids from Vendors and their bids are required to meet a minimum score. Any Vendors meeting the minimum score will have their EFCDs evaluated through a Benchmark test creating an overall Vendor score. These overall scores together with the evaluation process will be used to determine the winning supplier. The successful Vendor will complete the required changes to the EFCDs based on the requirements and work with RCMP staff to ensure the requirements are clearly understood and effectively implemented. Consequently, there will be some Vendor project management activities to complete the required changes and coordinate discussions with RCMP staff. Design document reviews can be used as part of the approval process; however, the RCMP's focus is on approving the EFCD's functionality and operation. (I)
4. Additionally, there is no plan to have Factory Acceptance Testing (FAT) for EFCDs. Any changes to EFCDs will follow an RCMP approval process to verify all requirements are satisfied. This process is expected to be similar to the RCMP certification process with user acceptance testing added to ensure the changes operate as required on the EFCDs and receive a recertification (if required) indicating they are ready for Production use. This approval process may be adjusted, as required. The RCMP will ensure Subject Matter Experts (SMEs) are available in a timely manner to clarify requirements, review and/or approve documentation, functional user interface screens, or interim versions of the EFCD updates (e.g. agile method) as required. (I)
5. The Vendor shall provide the goods and services described herein, in accordance with the terms and conditions of the contract resulting from this SOR, that will enable the RCMP/GC/CPMGs to continue efficient, effective and secure RTID System processing that supports the requirements included in this SOR and its accompanying documents. (M)

6. Mandatory requirements are marked with “(M)” at the end of a paragraph or an “M” in tables where mandatory requirements are listed identified using the terms “must”, “shall” or “will”. (I)
7. Rated requirements are marked with “(R)” at the end of a paragraph or an “R” in tables where rated requirements are listed. The wording used to identify these rated requirements is “should”, “could” or “may”. (I)
8. Information items are marked with “(I)” at the end of a paragraph. (I)
9. A List of Definitions is included Attachment A-3 (I).

1.2 ICD / NMSO Background And Related Information

1. RCMP’s RTID System supports the electronic submission, search and response to fingerprint search transactions based on NPS-NIST-ICDs. In support of the RTID System, the RCMP identified a need to establish a procurement mechanism to allow RCMP and GC Federal Departments a means to procure EFCDs to enable the creation, submission, printing, storage, and response processing of NPS-NIST-ICD compliant transactions. The NMSO created through this previous process will expire in October 2020; consequently, a replacement NMSO is required to support the continuing requirement for EFCD processing by the RCMP and GC. (I)
2. There is also no requirement for bidders to support the Immigration Enrolment Submission (IMM) transaction prior to bidding. (I)
3. The Vendor must be able to support the IMM transaction and the Deportee workflow requirements stated throughout this SOR and its accompanying documents as well as be capable of the supply, maintenance, and support of EFCDs that successfully process IMM transactions and the Deportee workflow. Supporting the IMM and Deportee requirements, if implemented, will be part of a Task Authorization after contract award. (M)
4. The following three (3) existing 1.7.8 ICDs were merged into one ICD as NPS-NIST-ICD 1.7.8 Revision 1.6: (I)
    a. the current Revision 1.3;
    b. AFIS Renewal RFP Revision 1.4; and
    c. the internal Cardscan ICD.

1.3 High-level Requirement

1. This requirement includes establishing a standing offer for one (1) Vendor. Consequently, the GC is expecting very competitive pricing for the devices included in the NMSO and the evaluation criteria reflects this expectation. (I)

2. With the bid submission, the Vendor must provide RCMP Letters of Certification for each Type of Transaction (TOT) for which they have certifications indicating that they have at least two (2) EFCDs, both a Livescan (capable of capturing Rolled/Plain/Palm and ID Flat prints) and Cardscan device (capable of capturing Rolled/Plain/Palm and ID Flat prints), certified by the RCMP to support all of the following TOTs for the NPS-NIST-ICD 1.7.8 Rev 1.6 (included as a compliancy document herein): (M)

    a. Criminal Tenprint Transaction Retain Yes (CAR-Y);

    b. Criminal Tenprint Transaction Retain No (CAR-N);

    c. Refugee Transaction (REF); and

    d. Miscellaneous Applicant Civil (MAP).

3. The NPS-NIST-ICD 1.7.8 Rev 1.6 was formally published in February 2019 after addressing comments received from the Letter Of Interest (LOI) (I).

4. If required, the EFCDs of the selected Vendor must be ready for RCMP recertification after completing the changes required to support the requirements, as stated in this SOR and its accompanying documents, within six (6) months of contractor selection or they may be removed from the NMSO as noncompliant; and the next most qualified bidder may be considered. RCMP is solely responsible for determining whether recertification is required based on the changes completed by the Vendor. (M)

5. The requirement must include the supply, maintenance, and support of EFCDs (Livescan and Cardscan) for the RCMP, GC, as well as all CPMGs. (M)

6. The requirement must include the supply, maintenance, and support of SMTP-SPOI Servers when there is more than one (1) EFCD at an agency, if required. (M)

7. RCMP requires that agency/sites with more than five (5) EFCDs use a single point of contact for communication with the RTID System, with rare exceptions when an agency/site can have more than one (1) EFCD without an SMTP-SPOI server. (I)

8. These EFCDs must be capable of supporting the Deportee workflow, which is an altered CAR-Y workflow that efficiently enables the creation of a CAR-Y when processing deportee charges. This must include creating, transmitting, storing, receiving and processing responses compliant with the NPS-NIST-ICD 1.7.8 Rev 1.6 for deportee charges. All the applicable CARY requirements stated in this SOR and its accompanying documents apply to the Deportee workflow. The Deportee workflow is essentially a CARY workflow with the charges automatically defined (refer to Annex D for details). (M)

9. These EFCDs must support the ability to receive a NIST packet from a Records Management System (RMS) / Digital Mugshot System (DMS) containing Type-1, Type-2 data and Type-10 images, and then use this data to create NPS-NIST-ICD 1.7.8 Rev 1.6 compliant transactions for submission through the EFCD to the RTID System. The EFCD must capture the biometric images, create a properly formed NPS-NIST-ICD 1.7.8 Rev 1.6 transaction, transmit the transaction to the RTID System and support all processing for the transaction based on the TOT even though some of the data was received through an RMS/DMS. (M)

10. These EFCDs must support the ability to send a response back to an RMS/DMS, which includes the original DCN, such as a NIST packet to indicate completion of the transaction (e.g. ACKT, SRE). Refer to Annex D for detailed workflow requirements. (M)

11. The EFCDs must operate with Windows 10 Operating System (OS). (M)

12. All Windows servers and Livescans/Cardscans must be maintained with the latest updates for the OS; and the latest Anti-Virus (AV) DAT files and AV policies. For the Livescans/Cardscans and any Windows servers, the maintenance of the latest updates must be through RCMP's/GC's/CPMGs' automated Windows Server Update Services (WSUS) and McAfee ePolicy Orchestrator (ePo), unless the department does not have WSUS and ePo. The Vendor solution must interface with, and automatically process data received from RCMP's/GC's/CPMGs' WSUS and ePo. (M)

13. These requirements include the supply, support, and maintenance of ruggedized Kiosks to support Livescan operations in non-office environments. (M)

14. These requirements shall include the replacement/upgrade/reuse of all components and subsystems where applicable. (M)

15. This requirement shall include the support and maintenance of all EFCDs in a manner that provides a secure operating environment within the RCMP/GC/CPMGs/Shared Services Canada (SSC) infrastructure. (M)

16. This requirement shall include user training on the EFCD as requested. (M)

1.4 Document Organization

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

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

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

   a. this Appendix A describes the:

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

      ii. scope of supply by the Vendor and the RCMP/SSC;

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

      iv. high-level requirements and the key areas to be delivered by the Vendor;

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

      vi. ongoing support requirements to be provided; and

      vii. deliverables that are to be completed by the Vendor;

   b. Annex A describes the current architecture within which the EFCDs must effectively operate;

   c. Annex B describes the detailed technical requirements for the EFCDs;

   d. Annex C describes the detailed support and maintenance requirements for the EFCDs;

   e. Annex D describes the detailed workflow requirements for the EFCDs;

   f. Annex E lists all Government Furnished Equipment (GFE) available for use by the Vendor;

   g. Annex F describes the Livescan/Cardscan Interface Specification that allows User Interface (UI) data fields to be provided to the Livescan/Cardscan from an agency related system;

   h. Attachment A-1 identifies the C-216 printed fingerprint forms that must be produced by the EFCD as stated throughout this SOR and its accompanying documents; and

   i. Appendix E describes the Call-up Limitations / Process;

   j. Appendix J describes the Evaluation Plan and Criteria; and

   k. Appendix K describes the Requirements Traceability Matrix.

1.5 Document Purpose

1. The purpose of this SOR is to present the RCMP/GC/CPMGs functional, technical, support and maintenance requirements of the EFCD NMSO to be delivered by the Vendor. (I)

2. The requirements contained in this document and referenced in other attached documents will be used by Canada to select one (1) Vendor to establish a standing offer for hardware and software that is to be installed, configured, supported, maintained and made fully operational according to the requirements stated throughout this SOR and its accompanying documents. (I)

3. This document provides the requirements that must be supported to enable the RCMP, GC and CPMGs to effectively create, submit and process all TOTs identified in the NPS-NIST-ICD 1.7.8 Rev 1.6 as well as the IMM transaction and its associated response TOTs in NPS-NIST ICD 2.1.1 Revision 3.0, for Immigration External Contributor. This document also details the functional requirements, technical requirements, interface specifications, performance, capacity requirements, quality, security, availability, integrity, training, implementation, support and maintenance requirements that the Vendor must satisfy. (M)

1.6 Compliancy Standards and Reference Documents

1.6.1 COMPLIANCY DOCUMENTS FORMING PART OF STATEMENT OF WORK

1. The following documents form an integral part of this SOR. The Vendor must propose a solution that complies with the content of all the listed documents in this subsection. (M)
    a. NPS-NIST ICD 1.7.8 Revision 1.6 for External Contributors, (RDIMS #43697) (minor updates since publishing) and its associated Supplemental Document For NPS-NIST-ICD 1.7.8 Revision 1.6 (RDIMS #45259);
    b. NPS-NIST ICD 2.1.1 Revision 3.0, for Immigration External Contributor (RDIMS #40361) IMM related requirements only;
    c. SMTP NIST Message Guidelines Version 4.1 (RDIMS #21047);
    d. American National Standards Institute National Institute of Standards and Technology – Information Technology Laboratory ANSI NIST-ITL 1-2011 - update 2015;
    e. Electronic Biometric Transmission Specification (EBTS), Criminal Justice Information Services, FBI, Version 10.0, September 2014 where applicable references are identified throughout this SOR and its accompanying documents and including:
        i. Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications, Appendix F, and
        ii. FBI IAFIS Image Quality Specification for Type-10 (Photo) Records Appendix K;
    f. WSQ Gray Scale Image Compression Specification, IAFIS-IC-0110 (V3.1), Federal Bureau of Investigation, Version 3.1 October 04, 2010;
    g. FBI Biometric Specifications (BioSpecs) - Certified Products List (https://www.fbibiospecs.cjis.gov/Certifications);
    h. Council Regulation (EC) No. 2252/2004 on standards for security features and biometrics in passports and travel document issued by Member States;
    i. ISO/IEC 19794-5:2011, Biometric Data Interchange Formats – Part 5: Face Image Data;
    j. ISO/IEC 19794-4:2011, Biometric Data Interchange Formats – Part 4: Finger Image Data;
    k. ISO/IEC 14443, Identification Cards – Contactless integrated circuit(s) cards – Proximity Cards;
    l. ICAO NTWG, User of Contactless Integrated Circuits In Machine Readable Travel Documents, Technical Report, Version 3.1, 16 April 2003;
    m. RTID Secure File Transfer Technical Architecture (RDIMS #39435) (provided after nondisclosure agreement signed); and

n. PART XIV of the Treasury Board Of Canada Secretariat "Occupational Safety and Health Directive", Section 14.12.1 "Manual Handling". http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_119/oshd-dsst/oshd-dsst_e.asp.

1.6.2 REFERENCE DOCUMENTS

1. The following documents are for reference purposes. The Vendor should use these documents to understand RTID related information and ensure the Vendor's solution effectively and efficiently supports these preferred processing capabilities. (R)

   a. Scanner Block Certification Specifications v5.0 (RDIMS #43381);

   b. Certification Process For Electronic Fingerprint Capture Device Systems Version v2.00 (RDIMS #45157);

   c. Best Practices for the Implementation of Civil Efficiencies of Fingerprint Capture Device Workflows, Version 1.7 (RDIMS #45311);

   d. Best Practices for the Capture of Charge Information In Support Of NPS-NIST-ICD V1.7.8 v2.00 (RDIMS #24626);

   e. RTID Introduction for Agencies (RDIMS #19085);

   f. RTID Technical Guidelines for Agencies (RDIMS #19086); and

   g. RTID Security Policy and Guidelines for Non-Law Enforcement Agencies (RDIMS #15761).

1.7 Scope of Supply

1. This section outlines the scope of supply for the Vendor and the corresponding supply by the government department. This is not intended to be a comprehensive list. This section is intended to provide the Vendor with an understanding of the scope of the requirements without reviewing all documentation included in this SOR to determine their potential interest in responding to this NMSO. The Vendor must supply all goods and services required to satisfy all the requirements stated in this SOR and its accompanying documents unless otherwise stated. (M)

1.7.1 THE VENDOR

1.7.1.1 Included in Supply

1. Hardware, Operating System (OS), software and all other components/deliverables (excluding GFE) required to provide fully operational EFCDs or SMTP-SPOI Servers or replace existing EFCDs or SMTP-SPOI Servers that satisfies the requirements as stated throughout this SOR and its accompanying documents based on the NMSO request by the government department. (M)

2. **Note**: Software means any drivers, application, third-party or any other software required by the Vendor to provide a solution that satisfies all the requirements stated throughout the SOR and its accompanying documents. (I)

3. The EFCDs and SMTP-SPOI Server must also comply with server/workstation security requirements of the government department. (M)

4. All software and/or hardware changes required to the GFE to support the requirements stated in this SOR and its accompanying documents. The Vendor must describe in detail how the GFE will be utilized in the Vendor's solution and what changes are required, if necessary. (M)

5. Testing to ensure all the Vendor functionality shall be fully operational between all Vendor components; and between the Vendor components and the RTID System. (M)

6. Training on an as-required basis through a Task Authorization. (M)

7. All other deliverables and services required by the Vendor that will satisfy the requirements stated in this SOR and its accompanying documents. (M)

8. All the corporate and management infrastructure and staff to support providing NMSO devices in a timely manner to RCMP/GC/CPMGs departments. (R)

1.7.1.2 Vendor Dependencies

1. RTID is a fully-operational system based on the ICDs identified in this SOR. The Vendor's solution must fully support the compliancy documents as stated in Section 1.6.1 Compliancy Documents Forming Part of Statement of Work. The RTID System has been available to test the Vendor's solution based on the ICDs as of December 2018; therefore, there are no RCMP RTID System dependencies to test all requirements stated throughout this SOR and its accompanying documents, unless noted. (M)

2. Any Vendor components must successfully pass RCMP Departmental Security Branch (DSB) Vulnerability Assessments (VA) before they can be connected to the any RCMP/GC/CPMGs Network. (M)

3. The Vendor must provide the fully operational EFCDs and SMTP-SPOI Servers, ready for re-certification/acceptance testing, and fully supporting the requirement stated throughout this SOR and its accompanying documents within six (6) months of contract award. (M)

4. The GC prefers the Vendor provide the fully operational EFCDs and SMTP-SPOI Server, ready for re-certification/acceptance testing, and fully supporting the requirement stated throughout this SOR and its accompanying documents as quickly as possible after contract award. (R)

5. Note: Time will be available to built and test the installation files (e.g. Batch, MS Installer (MSI)) that will be used for the Microsoft's System Center Configuration Manager (SCCM) package to be built in the RCMP environment, while the re-certification/acceptance testing is occurring. (I).

1.7.1.3 Vendor Configuration Management Tools and Process

1. The Vendor must use Configuration Management tools and processes to maintain the software and configuration changes completed throughout the life of this NMSO. (M)

2. The tools and processes should be included in the response to this RFSO and described to a level of detail that clearly identifies an effective, efficient and proven method to manage the NMSO specific software/configurations constituting the Vendor's proposed solution. (R)

3. The Vendor must maintain an NMSO activity report that records the Vendor's supply activities throughout the life of the NMSO. (M)

1.7.1.4 Vendor Documentation

1. The Vendor should provide sufficient detailed design documentation that explains all aspects of the Vendor's proposed solution and how the design/architecture of the proposed solution satisfies the requirements stated in this SOR and its accompanying documents. The Data Item Descriptions in Section 6 describes the documentation that should be provided by the Vendor. It is the Vendor's responsibility to include the documentation, in response to this RFSO, required to demonstrate that all requirements are satisfied. The documentation provided will be used by the GC to evaluate the proposed solution. (R)

1.7.1.5 Benchmark Testing

1. At no cost to Canada, benchmark testing must be completed at RCMP offices in Ottawa, Ontario, Canada. It is expected that this benchmark testing will occur at RCMP offices located at 1200 Vanier Parkway; however, it could be completed at a different RCMP office in Ottawa, Ontario, Canada. (M)
2. The benchmark testing will take approximately three (3) days per Vendor. The benchmark testing will be part of the NMSO evaluation process. (R)
3. The Vendor is responsible for providing and configuring a benchmark configuration of the proposed Livescan solution, to be used in the benchmark testing, to the RCMP designated Ottawa, Ontario, Canada office for evaluation purposes. Failure to provide a solution would result in a zero (0) score for the benchmark portion of the evaluation. (I)
4. The RCMP benchmark data will include fictitious demographic data fields and fingerprints from RCMP test subjects. (I)
5. The designated Public Services and Procurement Canada (PSPC) Procurement Officer will provide notification of the benchmark test date to the Vendor allowing the Vendor five (5) working days to deliver the Livescan for the scheduled benchmark test. The benchmark Livescan must be delivered to RCMP offices in Ottawa, Ontario, Canada. (M)
6. This benchmark test scheduling and other related details will be discussed further with the Vendors that successfully reach the benchmark testing stage. (I)
7. If Canada determines during the benchmark test that the Vendor's proposed solution does not meet the mandatory requirements, where the Vendor's proposal stated it would be supported within the scope of the benchmark test of this solicitation, the Vendor's proposal may be declared noncompliant and be disqualified. (I)
8. Canada may, as a result of any such demonstration, reduce the score of the Vendor on the rated requirements, if the benchmark test indicates that the score provided to the Vendor on the basis of its written proposal is not validated by the benchmark; where the Vendor's proposal stated it would be supported within the scope of the benchmark test. This is to ensure a Vendor's score for rated requirements is accurately determined. No Vendor's score will be increased as a result of any demonstration during the benchmark. (I)
9. If a Vendor 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 Vendor (e.g., acts-of-God, war, terrorism or widespread power outages) in which case PSPC may establish a revised schedule based on the situation. (I)
10. Refer to Appendix J, Evaluation Plan and Criteria for additional details concerning the benchmark testing. (I)

1.7.1.6 Exclusions

1. There are no specific exclusions within the context of this NMSO. (I)

1.7.2 RCMP/GC/CPMGs

1.7.2.1 Included in Supply

1. GFE servers and workstations procured by the RCMP/GC/CPMGs through a GC NMSO or other means, existing flatbed scanners, existing printers and any other components usable by the Vendor's proposed solution. Refer to Annex E which includes all components provided as GFE. (I)
2. Network devices such as Layer three (3) switches and stackable switches. The Layer three (3) switches include Load Balancing (LB) capabilities, Secure Sockets Layer (SSL) termination and communication between the GC sites using the Vendor's EFCDs and the RCMP's RTID System. (I)
3. Communications Security infrastructure. (I)
4. McAfee ePolicy Orchestrator (ePo) services (where available) and McAfee client software as required. (I)
5. Internal/external communications infrastructure. (I)
6. Workstation cabling between Livescans/Cardscan and RCMP/GC/CPMGs Local Area Network (LAN) drop. (I)
7. Technical support for installation at RCMP/GC/CPMGs facilities. (I)
8. NPS-NIST Server (NNS) functionality including all interface capabilities based on the ICDs. (I)
9. Project management of a large number of EFCD, within which the Vendor activities would be included. However, any government department may choose to complete a Task Authorization for the Vendor to perform project management. (I)
10. Coordinate Vendor access to Subject Matter Experts (SMEs) as required. The RCMP will ensure required resources are available to respond to Vendor questions/actions in a timely manner. (I)
11. Approval authority for decisions, approvals and sign-off required by Vendor. (I)
12. NMSO device defects will be tracked through RCMP's defect reporting process. (I)

1.8 Terminology Clarification

1. The phrase, “any OS and/or software upgrade completed through the execution of the work required to complete this SOR 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/GC/CPMGs 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 Vendor, as required. As well, VAs can be performed as soon as the Vendor has a device configured to support the NMSO requirements to ensure vulnerabilities are identified as early as possible in the process; therefore, enabling corrections as soon as possible. (I)
2. In the context of this SOR, the term, “component”, means any identifiable part of the Vendor’s solution required to provide a fully operational solution that satisfies all the requirements throughout this SOR and its accompanying documents. For example, components might include servers, workstations, printers, scanners, cameras, databases, firmware and any other devices/products required to provide a fully operational device. (I)
3. The term, “EFCD”, refers to computer-based systems that digitize biometric images (fingerprints, palm prints, photo) and includes a means to enter biographic, demographic and/or criminal information (e.g. Livescan, Cardscan). (I)
4. The term, “Livescan”, represents a standalone model, desktop model or a portable model (Laptop) device unless specifically stated otherwise. A Livescan is an EFCD utilizing a scanner block and camera to perform a live capture of a subject’s biometric images. It may also have other components (e.g., printer) that operate with the Livescan to provide a comprehensive solution that satisfies a specific NMSO clients requirements. (I)
    a. Standalone – components integrated within a protective cabinet (i.e., Ruggedized Kiosk cabinet). Components include a Central Processing Unit (CPU), monitor, keyboard, mouse, Uninterruptible Power Supply (UPS), foot pedal, magnetic stripe reader, 2D barcode reader, digital camera and a fingerprint capture scanner that supports the capture of rolled/plain fingers, palms, and ID Flats. This configuration would normally be situated within a criminal law enforcement environment. A printer will also be part of the standalone component configuration but will not be contained within the protective cabinet;
    b. Desktop - components include a CPU, monitor, keyboard, mouse, UPS, a digital camera with tripod and fingerprint capture scanner that supports the capture of rolled/plain fingers, palms, ID Flats. This configuration could optionally include a foot pedal, magnetic stripe reader, 2D barcode reader and printer. This configuration could also be adjusted to use a scanner block that only includes rolled/plain fingers and ID Flats or a scanner block that only includes only ID Flats. This configuration would not normally be situated within a criminal law enforcement environment; and

c. Portable – components include a laptop computer, mouse, onboard power supply, fingerprint scanner that supports the capture of rolled/plain fingers and ID Flats (no palms) or ID Flats only, and a digital camera with tripod and a reinforced travel case with retractable handle and wheels. This configuration could optionally include a foot pedal.

5. The term, “Cardscan”, represent a desktop model device unless specifically stated otherwise. A Cardscan is an EFCD utilizing a flatbed scanner to capture a subject’s biometric images from a paper form. It may also have other components (e.g., printer) that operate with the Cardscan to provide a comprehensive solution that satisfies a specific NMSO clients requirements. (I)

6. The term, “SMTP-SPOI Server”, represents a device that provides a single point of communication between an NMSO client site with multiple EFCDs and the RTID System. The SMTP-SPOI Server will support transactions to/from multiple agency Livescans or a combination of Livescans and Cardscans and the RTID System. The SMTP-SPOI Server may also have an optional transaction case management component that will manage all transactions it receives from internal devices as well as responses from the RTID System. (I)

7. The term Operational Livescan User (OLU) refers to a person or persons who perform day-to-day enrolments, resubmissions and review search results in an operational environment. This acronym also applies to Cardscan operators. (I)

8. The term Operational Livescan Administrator (OLA) refers to a person or persons who have administrative privileges on the Livescan device to perform as and when required application administrative activities. These activities include at least the following: changing application configuration parameters, backing up systems, setting auto-deletion parameters for file deletion, adding users, reviewing logs, reports, troubleshooting and managing user privileges. This acronym also applies to Cardscan operators. (I)

9. The term Information Technology (IT) Support refers to a person or persons who have administrative privileges on the Livescan device to perform IT support and maintenance activities such as installing software, changing the operating system and reconfiguring the device upon which the Livescan application operate. This acronym also applies to Cardscans. (I)

10. All rated requirements identified as met or will be met in the Contractor’s proposal become mandatory requirements for the final version of the EFCD(s) / SMTP-SPOI. (I)

11. The terms “charge table” and “Federal Statutes Table” are synonymous. (I)

12. The terms Contractor, Vendor and Offeror are synonymous. (I)

13. A configurable parameter means a parameter that can be set by an authorized user that changes the behaviour/functioning of the EFCD without requiring the application to be recompiled/rebuilt/recreated. Once the configurable parameter is changed, the new behaviour/functioning must be automatic or only require a restart. (I)

1.9 Bilingualism

1. The Vendor's NMSO Livescan/Cardscan solution shall be delivered in Canadian English and Canadian French at the user interface level. (M)

2. The Vendor should describe how language is implemented architecturally in their solution. (R)

3. English and French must not appear on a screen at the same time, unless otherwise indicated in this SOR and its accompanying documents, and users shall sign in with either one of the two languages. (M)

4. The Vendor's NMSO Livescan/Cardscan solution shall be functionally equivalent in both official languages (Canadian English and Canadian French) according to Canadian Federal Government standards. The NMSO Livescan/Cardscan solution must adhere to the following Acts and Policies: (M)

    a. Official Languages document entitled *Official Languages Act* (R.S.C., 1985, c. 31 (4th Supp.)) at http://laws-lois.justice.gc.ca/eng/acts/O-3.01/; and

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

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

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

7. The NMSO Livescan/Cardscan solution shall permit users to select their default language of operation as part of their profile. (M)

8. The EFCD Help Files must be in Canadian English or Canadian French based on login language selection. (M)

9. The EFCD workflow functionality must be identical irrespective of language selected. (M)

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

11. The ICDs in Section 1.6 (Compliancy Standards and Reference Documents) contain the code values that are applicable to each input field. (I)

12. The NMSO Livescan/Cardscan solution shall make a French and English description available for each code table value. (M)

13. The NMSO Livescan/Cardscan solution shall display the description associated with a code table value in the language currently selected by the user. (M)

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

15. The Vendor must provide the translation services for the Main Screen, French Workflow Screens, Help Files and user/administrator documentation materials. (M)

16. The Vendor must update their French translated documentation / workflows with any recommendations made by the RCMP, especially to ensure the format of the French GUI screens are acceptable. (M)

17. The Vendor must provide any translated material as soon as possible to allow RCMP to review and provide feedback and corrections. The material must be provided at least fifteen (15) days prior to testing to allow the Vendor to make corrections prior to testing. (M)

18. The EFCD software shall support accented and special characters for the input/display of French data, in data fields where this is allowed (e.g., labels. messages, help files). (M)

1.10 Security And System Updates

1. The transmission of RTID data is considered Protected B. The Vendor must be experienced operating and supporting devices in a Protected B environment. The RTID System only allows Protected B connections with external devices such as Livescans/Cardscans. (M)

2. The software and document deliverables are considered Protected A. The Vendor must be experienced handling Protected A deliverables. Any exchange of software or documentation between the RCMP/GC/CPMGs sites and off-site Vendor resources must be exchanged securely in a manner acceptable to the RCMP/GC/CPMGs site. (M)

3. For security reasons, all equipment, provided by the Vendor must be physically located on RCMP/GC/CPMGs premises and used exclusively by the RCMP/GC/CPMGs resources or as required Vendor resources on the RCMP/GC/CPMGs premises. All sites certified to use a Livescan/Cardscan/SMTP-SPOI will have an RCMP approved secure connection for RTID communication. (M)

4. The RCMP/GC/CPMGs agency will provide access for Vendor resources, as required, to facilities necessary to provide support for the devices procured through this NMSO. This will include network access, unless otherwise stated as part of the support agreement, to support all NMSO devices by the Vendor for the specific RCMP/GC/CPMGs agency through a single physical location using approved remote access connectivity capabilities. That is, for RCMP/GC/CPMGs agencies, with multiple NMSO devices to support, the Vendor will be able to support all the devices through one RCMP/GC/CPMGs physical site specific to the RCMP/GC/CPMGs agency/department, unless the device requires a physical change (e.g. hard drive replacement). (I)

5. The Vendor must complete EFCD software updates/upgrades/corrections, and software installations on GFE, through SCCM. That is, the Vendor must provide the RCMP/GC/CPMGs with installation files (e.g. Batch, MSI) that can be used to automatically update/install the EFCD software through SCCM. (M)

6. Vendor support for RCMP/GC/CPMGs sites that do not support SCCM must be completed through an RCMP/GC/CPMGs approved remote connectivity tool (e.g., PC Duo) to access the device and provide support directly on the device remotely. The RCMP/GC/CPMGs department will allow this access through the department's device (i.e., workstation). (M)

7. The EFCD updates/upgrades/corrections must be allowed to be completed without any Windows OS configuration changes. That is, there must be no requirement to for the IT support staff to disable any OS features/applications (e.g. User Account Control, Backup) in order to complete the EFCD updates/upgrades/corrections. (M)

8. The Vendor must complete EFCD Charge Table updates through SCCM. That is, the Vendor must provide the RCMP/GC/CPMGs with installation files (e.g. Batch, MSI) that can be used to automatically update the EFCD charge table through SCCM. (M)

9. The Vendor EFCDs must provide an alternate method to manually update the Charge Table for those departments/agencies that do not use SCCM. (M)

10. If the manual update process for the Charge Table is used, it should be as automated as possible to minimize the number of steps and/or key strokes / mouse clicks required by the IT staff. The ideal solution is to use the same or similar installation files used for the automated updated through SCCM. (R)

11. The Vendor's EFCD must be able to operate with full capabilities with the EFCD installed with department/agency tools to manage the device (e.g. IBM EndPoint Manager Client). (M)

12. The Vendor must gain and maintain security clearances required by the specific government department, for a minimum of two (2) personnel, which enables the Vendor to provide the required support for the NMSO procured devices. Failure to achieve these security clearances will prevent the Vendor from supporting the specific department's NMSO devices and may cause the Vendor to be deemed noncompliant, which may require the contract to be terminated. (M)

1.11 Constraints

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

2. The Vendor's solution must include the option for ongoing support and maintenance by the Vendor. That is, once procured and after the one (1) year warranty period, the department must have the option to have the Vendor provide support and maintenance for the procured NMSO devices as stated throughout this SOR and its accompanying documents. (M)

3. Any changes that are made to the devices available throughout the existence of this NMSO, that potentially affects the device's security, must successfully pass a VA completed by RCMP's DSB or designated GC/CPMGs department. Software updates and simple software upgrades typically do not require a VA. It is at the sole discretion of the GC to determine if a device change affects the security of the device such that a VA is warranted. The Vendor shall be responsible for making the required changes to successfully pass a VA. (M)

4. The Vendor is expected to inform the GC of anything that might improve the overall solution requested in this SOR; and/or the efficiency with which the solution might be implemented. The GC has sole responsibility for deciding to use any suggestions presented by the Vendor. (I)

2. BACKGROUND

2.1 General

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

2. RCMP/GC/CPMGs departments currently have many existing EFCDs that have been procured through various means that currently submit to the RTID System. The components that constitute these EFCDs may be considered GFE for this NMSO RFSO. Refer to Annex E for details concerning the GFE. (I)

3. Figure 2-1: High-Level EFCD/SMTP-SPOI/RMS/DMS Architecture depicts a high-level view of typical Livescan/Cardscan/SMTP-SPOI/ RMS/DMS connectivity models that communicate with the RTID System. Not all possible configurations are identified herein. (I)

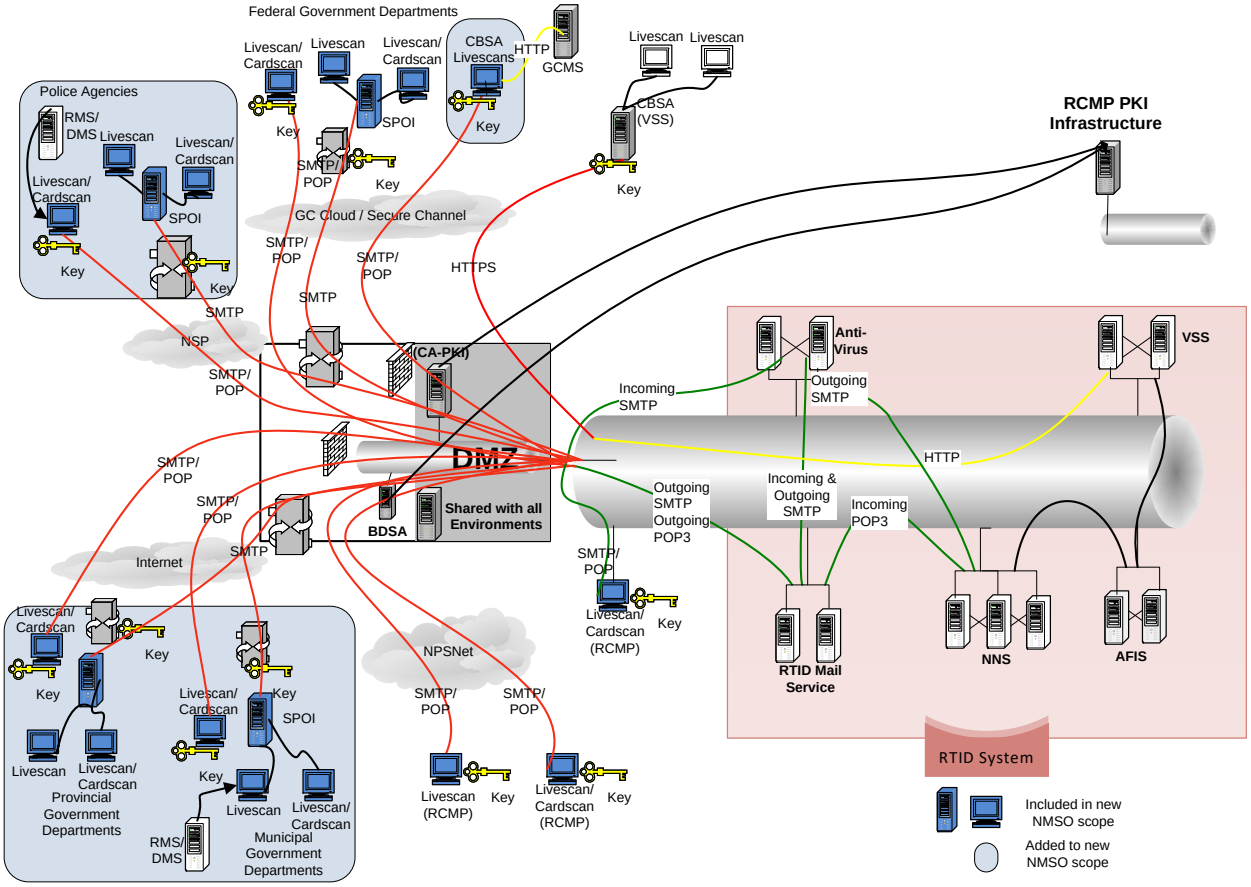


Figure 2-1: High-Level EFCD/SMTP-SPOI/RMS/DMS Architecture

4. Annex A describes additional details concerning the current architectures, for RCMP/GC/CPMGs departments, that the Livescan/Cardscan/SMTP-SPOI must operate within. (M)

5. The following is a high-level description of the NMSO applicable devices depicted in the current high-level RTID architecture diagram: (I)

   a. RTID submission devices:

      i. Cardscan, Livescans, and SMTP-SPOI servers submit to RTID based on the NPS-NIST ICDs for External Contributors. These submission devices are owned and operated by RCMP/GC/CPMGs departments.

      ii. these devices all submit to the RTID System using SMTP and receive responses through either SMTP or Post Office Protocol (POP) email protocols;

      iii. these devices are located across Canada;

      iv. these devices connect through a secure connection established between the RTID System and the submitting agency; and

v. CBSA has a specific requirement to access the Global Case Management System (GCMS) from the Livescan/Cardscan to allow eight (8) fields to be automatically populated for the Livescan/Cardscan transactions. This capability is also available for other agencies for fields that may be applicable to them. Refer to Annex A for additional technical architecture details and Annex F for the Livescan/Cardscan Interface Specification details. The RCMP has already implemented a stub system (i.e. substitute for a full system) that can be used to test this Livescan interface.

3. REQUIREMENT

3.1 General

1. The following subsections describe the high-level requirements that must be satisfied by the NMSO RFSO devices. The additional detailed requirements that must be satisfied are described in the annexes attached to this SOR. (M)

2. The Vendor must provide all the Vendor software, hardware, OS, peripherals, third-party software, configuration and anything else required to create fully operational Production ready devices that function as stated in this SOR and its accompanying documents. (M)

3. GFE software and/or hardware may be used by the Vendor to provide fully operational Production ready devices that function as stated in this SOR and its accompanying documents. (R)

4. Some GFE software and hardware, as identified herein, must be reusable by the Vendor. (M)

5. The EFCDs and SMTP-SPOI servers must be able to operate effectively and efficiently with installed and configured features/capabilities such as SecureDocs, Bit Locker or other RCMP/GC/CPMG approved encryption software and/or DeviceGuard. (M)

6. It is preferred that the EFCD provide an on screen visual indication of the status of the connected peripherals that effectively shows that the peripheral is ready for use (e.g. scanner, camera, printer). (R)

7. All available Vendor EFCD and SMTP-SPOI capabilities such as reports that can be generated, printing features, or any other functionality must be available and operational on the EFCDs provided to the RCMP/GC/CPMG as part of the contract resulting from this solicitation, at no additional cost. That is, capabilities/functionality available on the Vendor's EFCD or SMTP-SPOI server, regardless of whether it is part of the COTS product or a configurable feature must be available for the RCMP/GC/CPMG EFCDs. (M)

3.2 Key Areas to be Delivered

1. The six (6) key areas that the Vendor must be able to provide under this SOR are Livescans/Cardscans, SMTP-SPOIs, ruggedized Kiosks, and support and maintenance of all components included in the scope of this SOR and its accompanying documents. (M)

2. Additionally, the Vendor must allow RCMP/GC/CPMGs to procure future compliant devices within the scope of this NMSO (i.e. any Vendor device capable of capturing biometrics and related data). (M)

3. The Vendor's solutions must operate effectively in the RCMP/GC/CPMGs architecture. Annex A describes the architecture within which the Vendor's solutions must operate. (M)

4. The Vendor's solutions must support everything in the current architecture, Annex A. That is, the RCMP/GC/CPMGs security/network architecture will not be altered to support an inefficient or less secure EFCDs/SMTP-SPOIs. (M)

5. The proposed EFCDs must be able to replace the existing EFCDs or replace only specific components of existing EFCD such as software, workstation and/or monitor. Refer to Appendix J Evaluation Plan and Criteria and Annex E to Appendix A - Government Furnished Equipment for details. (M)

6. If necessary, portions of the security architecture of the RCMP/GC/CPMGs can be explained; however, this is not expected to be necessary. This additional security architecture can only be provided upon request, and after a nondisclosure agreement is signed for anyone requiring a briefing. This briefing will only occur at RCMP/GC/CPMGs offices. The Security architecture will not be presented in this SOR. Only a high-level description of the Security architecture is included in this SOR to provide sufficient information that allows the Vendor to determine their interest and ability to respond to this SOR. Any potential Vendor would be expected to only need to know the level of security architecture provided herein to submit a proposal. (I)

7. The Vendor's solutions must use the ports identified in Annex A and in this SOR and its accompanying documents to communicate with the RTID System. (M)

8. The Vendor's solutions must use the ports identified in Annex A and in this SOR and its accompanying documents to communicate between EFCDs and SMTP-SPOIs. If any devices require different ports to communicate between the EFCDs and the SMTP-SPOI, it might be considered an acceptable difference providing it shall not create a vulnerability that is unacceptable to the RCMP/GC/CPMGs. Using different ports than identified in Annex A must be approved by RCMP's DSB prior to submitting a bid or the Vendor risks being noncompliant. RCMP is solely responsible for determining whether any aspect of the Vendor's proposed solution creates a vulnerability. (M)

9. The Vendor must also provide training and ongoing support for all the key areas, as required. (M)

10. There are many EFCD components (e.g., workstations, servers, printers, scanners, Kiosks) that have been recently procured by the RCMP/GC/CPMGs departments. These components are considered GFE for this NMSO RFSO and they are listed in Annex E. (I)

11. The EFCDs must operate with Windows 10 desktop Operating System (OS). (M)

12. Any costs associated with upgrading the GFE servers or workstations to satisfy the technical, functional or performance requirements of this SOR will be solely the responsibility of the RCMP/GC/CPMGs; however, the required changes must be identified in the Vendor's proposal. The Vendor's proposal must explain what GFE can be reused together with the Vendor's components and how the GFE will be reused. (M)

13. Any new or modified servers or workstations must successfully pass RCMP/GC/CPMGs approval before the device can be installed and used on the RCMP/GC/CPMGs network. (M)

14. All Windows servers or Livescans/Cardscans 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/GC's/CPMGs' automated Windows Server Update Services (WSUS) and McAfee ePolicy Orchestrator (ePo), unless the department does not have WSUS and ePo. The Vendor solution must interface with, and automatically process data received from RCMP's/GC's/CPMGs' WSUS and ePo. (M)

15. All non-Windows servers should be described in detail to allow the GC to determine the effectiveness of the solution to satisfy the requirement to maintain the servers with the latest updates for the OS; and the latest Anti-Virus (AV) DAT files and AV policies; as well as the support procedures for updates that are not automated. (R)

16. The Vendor will be responsible for the support and maintenance of new components and replaced/upgraded components of the Vendor's solution. For example, if the Vendor replaces the existing Livescan/Cardscan software on a workstation, the Vendor will be responsible for the support and maintenance of the software and the RCMP/GC/CPMGs department will be responsible for the support and maintenance of the hardware, unless otherwise agreed to with the Vendor. (M)

17. If the Vendor cannot replace the software with its own, and provide the support and maintenance stated throughout this SOR and its accompanying documents, then RCMP reserves the right to sole source the on-going maintenance and Change Requests (CRs) with the previous vendor in order to reduce costs. (M)

18. If the Vendor is not willing to replace the software with its own, and provide the support and maintenance stated throughout this SOR and its accompanying documents, then RCMP reserves the right to sole source the on-going maintenance and Change Requests (CRs) with the previous vendor in order to reduce costs; and/or may deem the Vendor non-compliant and terminate the contract. (M)

19. The RCMP/GC/CPMGs department may also request that the Vendor provide support and maintenance related to GFE including coordinating replacement parts/upgrades from the hardware / operating system through a Task Authorization or through an adjusted support and maintenance plan. (R)

3.2.1 LIVESCANS/CARDSCANS

1. The Livescans/Cardscans must successfully operate, satisfying the requirements stated throughout this SOR and its accompanying documents, in the current architecture as described in Annex A. (M)
2. The Vendor's Livescan/Cardscan must: (M)
    a. for Livescans, support printing to FBI certified printers and generate the printed result with the appropriate fingerprint form based on the forms included in Attachment A-1 herein. That is, the Vendor's Livescan must print the data and form on the FBI certified printer, as required;
    b. include a scanner block (for Livescan) or flatbed scanner (for Cardscan) to scan fingerprints according to the requirements stated throughout this SOR and its accompanying documents;
    c. for Livescans, include a camera to take photos, with a lighting system that ensures the requirements stated throughout this SOR and its accompanying documents are satisfied (also refer to refer to Annex E ANSI NIST-ITL 1-2011 for additional details);
    d. include all software and hardware required to successfully operate as stated throughout this SOR and its accompanying documents;
    e. include printing results of a search returned to the Livescan/Cardscan to a printer; and
    f. include anything else required to fully satisfy the requirements stated in this SOR and its accompanying documents.
3. The Vendor shall be responsible for providing the required software necessary to satisfy all the Livescan/Cardscan requirements identified in this SOR and its accompanying documents and configure the Livescan/Cardscan with a DSB approved operating system that will successfully pass the DSB VA. (M)
4. The Vendor's Livescan and Cardscan software should be identical, except for variances to accommodate using a scanner block for the Livescan versus a flatbed scanner for a Cardscan and variances for supporting a camera. (R)
5. The Vendor's Livescan/Cardscan must support communicating with the Agency's RMS/DMS to receive photos and biographical data that can be used by the Livescan/Cardscan to send NPS-NIST-ICD compliant transactions. (M)
6. The Vendor's Livescan/Cardscan processing of the Agency's RMS/DMS photos and biographical data should be an efficient, effective and simple to use GUI that seamlessly fits into the associated workflow. (R)
7. The Vendor's printed forms must match as precisely as possible the forms included in Attachment A-1 herein for certified TOTs required to bid. (M)
8. Annex B identifies the Livescan/Cardscan detailed requirements. (I)
9. Note: The name and version of the tools used to perform the VAs can be provided upon request. (I)

3.2.2 SMTP SINGLE POINT OF INTERFACE (SMTP-SPOI) SERVERS

1. The RCMP only allows one interface to the RTID System from an agency's site. If an agency has only one Livescan or only one Cardscan, that single device can interface with the RTID System. If an agency has more than one device, then the RCMP requires that the agency install an SMTP-SPOI server. (I)

2. Annex B identifies detailed requirements that also apply to the SMTP-SPOI Server. (I)

3. The SMTP-SPOI Server must support transactions from multiple agency Livescans, or a combination of Livescans and Cardscans, to the RTID System. The SMTP-SPOI Server must also communicate response transactions received from the RTID System to the agency Livescan/Cardscan that initiated the transaction. (M)

4. The SMTP-SPOI email service must be able to save all existing SMTP-SPOI email, when an SMTP-SPOI is replaced, to a commonly readable format such as Adobe to ensure the historical record of email can be maintained if the Vendor's solution does not allow the existing SMTP-SPOI email to be used by the Vendor's SMTP-SPOI Server. (M)

5. The Vendor must be able to export all data from the Vendor's SMTP-SPOI Server to a readable form such as Excel spreadsheet, PDF or similar common form to ensure historical data can be maintained if the SMTP-SPOI Server is replaced at a later date. (M)

6. The SMTP-SPOI server must have an optional transaction case management component that will manage all transactions it receives from agency's Livescan/Cardscan devices and response transactions from the RTID System. (M)

7. The Vendor shall be responsible for providing the required software necessary to satisfy all the requirements identified in this SOR and configuring the SMTP-SPOI servers with a DSB approved operating system that will successfully pass the DSB Vulnerability Assessment (VA). (M)

3.2.3 RUGGEDIZED KIOSKS

1. The Vendor must provide ruggedized Kiosks that support the requirements stated throughout this SOR and its accompanying documents. (M)

2. The ruggedized Kiosks are used for Livescan operations that are provided in a non-office environment. (I)

3. The ruggedized Kiosks must support all Livescan requirements installed and configured in the Kiosk. (M)

4. The Vendor's ruggedized Kiosks must include a Canadian Standards Association / Underwriters Laboratories of Canada (CSA / ULC) approved protective cabinet (CAN/CSA-C22.2 NO. 60950-1-07 (R16)). (M)

5. The Vendor's ruggedized Kiosks must be equipped with sufficient electrical fan(s) to exhaust air from the cabinet housing to prevent all equipment from overheating and failure. (M)

6. The Vendor's ruggedized Kiosks must be lockable with proven record of securely operating in a controlled public area that secures all components to prevent them from being easily removed. (M)

7. The Ruggedized Standalone Livescan Kiosk solution detailed specifications are included in Annex B EFCD Detailed Requirements. (I)

8. RCMP's DSB must certify any new (i.e. not previously used in the RCMP/GC/CPMGs) ruggedized Kiosk cabinet to ensure it satisfies GC requirements before it can be used in the production environment. (M)

3.2.4 SUPPORT AND MAINTENANCE

1. Annex C identifies support and maintenance detailed requirements that apply to all components that are included in the SOR and its accompanying documents. (M)

2. The support and maintenance coverage must include on-site preventive maintenance and remedial hardware and software support as well as telephone or online support for all EFCDs and SMTP-SPOI Servers delivered hardware and software. (M)

3. The support and maintenance coverage must include any EFCDs as well as SMTP-SPOI Server application software upgrades. (M)

4. Support and maintenance coverage must begin at the end of the warranty period. (M)

5. Support and maintenance must include: (M)

    a. Call Center support between 0700 hours to 2000 hours (Eastern Standard Time), Monday through Friday;

    b. 1-800 phone support;

    c. if the Customer Support Center is not able to resolve the issue then the next level of support will respond to the site within an hour of the initial call from the site;

    d. twenty-four (24) hour on-site response time to the trouble site from the time a trouble call is logged where the site is located within or outside of 160 kilometers of an airport serviced by major commercial airlines;

    e. regular repair or replacement of failed parts and software maintenance / upgrades;

    f. the failed site must be back operational within 48 hours of the initial trouble call for sites located within 160 kilometers of an airport serviced by a major commercial airline;

    g. the failed site must be back operational within 72 hours of the initial trouble call for sites located outside of 160 kilometers of an airport serviced by a major commercial airline; and

    h. Bilingual Customer Service Support services and Field Technical Support services in English and French.

3.2.5 TRAINING

1. The Vendor must provide training on all user aspects of the Vendor's solutions. (M)
2. The Vendor should provide the quality, experience and training cost of the Vendor's trainers for evaluation. (R)
3. The Vendor should have an EFCD training guide that is well organized and shows an effective and efficient training plan that will ensure users and administrators can easily comprehend all capabilities of the EFCD. (R)
4. The Vendor must be able to provide training session for OLUs, OLAs and/or SMTP-SPOI server at each Call-up site in Canada, as required. (M)
5. The Vendor must prepare and submit for RCMP review and approval / modification, a draft Training Plan. (M).
6. The training plan should clearly explain how the Vendor's training approach will result in effective and efficient training for the users. (R)
7. The training plan must use the Train-the-Trainer approach. (M)
8. The Training Plan must include information on the scope, duration, and all information available on any printed material, videos, and online training aides that will be provided. (M)
9. The Vendor must modify the Training Plan based on RCMP comments, as required. (M)
10. The Vendor must provide OLU and OLA User Manuals as required for the Livescan, Cardscan, SMTP-SPOI server and for all related software 10 business days before the scheduled start of training in both hard (paper) and/or soft (PDF format) copy in English and French based on the Call-up. (M)
11. The Vendor must provide a minimum of a half (1/2) day of OLA training for up to four (4) individuals, and a half (1/2) day of OLU training for up to four (4) individuals. (M)
12. The Vendor must provide hardcopy and/or softcopy User Manuals in English or French as directed by the Call-up agency. (M)
13. The Vendor's trainer must be fluent in English or French as dictated by the call-up issuer/authority. (M)

3.2.6 FUTURE COMPLIANT VENDOR DEVICES

1. The Vendor must make available, to the resulting NMSO, any new types of devices (e.g., remote handheld fingerprint scanner) that the Vendor certifies to any NPS-NIST-ICD during the entire contract period. (M)
2. These future devices must be provided with most favoured customer pricing available for the RCMP/GC/CPMGs. (M)
3. The exact pricing for these future devices will be determined with PSPC. (I)

4. Any future devices, not currently market available (e.g., remote handheld fingerprint scanner), that are applicable for RCMP certification or could be certified should be identified. (R)

3.3 Hardware and Software

1. All non-GFE hardware proposed by the Vendor must satisfy the requirements stated in this subsection, its subsections and all the other requirements stated throughout this SOR and its accompanying documents. (M)

2. This hardware subsection includes the following subcategories: (I)
   a. EFCD Workstations;
   b. EFCD Laptops;
   c. SMTP-SPOI Servers;
   d. Scanner Blocks
   e. Flatbed Scanners;
   f. Printers;
   g. Touch Screen Monitors;
   h. Cameras; and
   i. Software.

3. To substantiate the hardware and software requirements listed below, the Vendor shall provide in its solution a description of the hardware and software and their interrelationship within each component (e.g., Livescan, Cardscan, SMTP-SPOI) including, as a minimum, for each COTS hardware and software component proposed for this NMSO: (M)
   a. item make, model and version number;
   b. the NPS-NIST-ICD compliance met;
   c. the ANSI/NIST compliance and other standards met;
   d. certifications and ratings achieved;
   e. customization required;
   f. recommended and minimum performance criteria and capacities;
   g. the internal/external electronic interfaces; and
   h. the security services implemented.

4. All Vendor hardware must satisfy RCMP/GC/CPMGs electrical specifications, including the voltage, amperage, electrical receptacle, and CSA / ULC certification. (M)

3.3.1 EFCD WORKSTATIONS

1. The Vendor EFCD workstations must satisfy all Livescan/Cardscan requirements stated throughout this SOR and its accompanying documents. (M)
2. The Vendor EFCD workstations must allow all required components (e.g., monitor, printer, mouse, scanner block) to be connected to create a fully operational EFCD that satisfies all Livescan/Cardscan requirements stated throughout this SOR and its accompanying documents. (M)
3. The workstation detailed specifications the Vendor EFCD workstations must meet are included in Annex B EFCD Detailed Requirements. (M)

3.3.2 EFCD LAPTOPS

1. The Vendor EFCD Laptops must satisfy all Livescan/Cardscan requirements stated throughout this SOR and its accompanying documents. (M)
2. The Vendor EFCD Laptops must allow all required components (e.g., printer, mouse, scanner block) to be connected to create a fully operational EFCD that satisfies all Livescan/Cardscan requirements stated throughout this SOR and its accompanying documents. (M)
3. The Laptop detailed specifications the Vendor EFCD workstations must meet are included in Annex B EFCD Detailed Requirements. (M)

3.3.3 SMTP-SPOI SERVERS

1. The Vendor SMTP-SPOI servers must satisfy all SMTP-SPOI requirements stated throughout this SOR and its accompanying documents. (M)
2. The Vendor SMTP-SPOI servers must allow all required connectivity (e.g., network connection, communication with Livescans/Cardscans, communication with RTID) to create fully operational SMTP-SPOI servers that satisfy all SMTP-SPOI requirements stated throughout this SOR and its accompanying documents. (M)
3. The Vendor SMTP-SPOI servers must include an SMTP email service that supports communication with RTID and communication with the agency's Livescans/Cardscans as required. (M)
4. All Vendor SMTP-SPOI servers must support the Network Time Protocol (NTP) to maintain clock synchronization through the RCMP/SSC/GC/CPMGs network devices. (M)
5. The Vendor SMTP-SPOI servers must support SNMP reporting to RCMP/SSC/GC/CPMGs system monitoring solution. This SNMP reporting must include automated system level monitoring capabilities, at the hardware and software application level, capable of producing SNMP traps/alerts when software or hardware faults are detected. The minimum SNMP reporting must include memory utilization, CPU utilization, disk utilization, key process failures and hardware faults. (M)
6. The SNMP reporting capabilities will be determined for specific NMSO procurements. (I)
7. The Vendor SMTP-SPOI servers must support High Availability (HA) capabilities to support intra-site fail-over. (M)
8. The HA capabilities will be determined for specific NMSO procurements. (I)
9. The SMTP-SPOI Server detailed specifications that the Vendor-proposed EFCD workstations must meet that are included in Annex B EFCD Detailed Requirements. (M)

3.3.4 SCANNER BLOCKS

1. The scanner blocks must be capable of capturing: (M)
   a. Tenprint rolled fingerprint images;
   b. Tenprint plain fingerprint images;
   c. Palms images (upper, lower, writers); and
   d. ID Flat images.
2. At least one scanner block must be capable of capturing prints at 500ppi and/or 1000ppi. (M)
3. Fingerprints captured at 1000ppi must downsample to 500ppi prior for inclusion in the NIST packet sent to RTID. (M)

4. Refer to Annex B for additional detailed requirements for the scanner blocks within each type of Livescan device. (I)

3.3.5 FLATBED SCANNERS

1. The Flatbed Scanners must be FBI certified and support the scanning requirements stated throughout this SOR and its accompanying documents. (M)
2. The Flatbed Scanners provided with the Cardscans shall meet, at a minimum, the Image Quality Specification (IQS) of Appendix F in the Electronic Biometric Transmission Specification (EBTS) Version 10 or later. (M)
3. The Flatbed Scanners must support all scanner capabilities necessary to support all scanning requirements for Cardscans. (M)
4. Refer to Annex B for additional detailed requirements for the Flatbed Scanners within Cardscan requirements. (I)

3.3.6 PRINTERS

1. The Vendor's solution must support both FBI certified printers and non-certified FBI printers to support printing requirements as stated throughout the SOR and its accompanying documents. (M)
2. The FBI certified printers provided shall meet, at a minimum, the Image Quality Specification (IQS) of Appendix F in the Electronic Biometric Transmission Specification (EBTS) Version 10 or later (for latent / ten print printers, latent / ten print display stations and latent and ten print scanners). (M)
3. Printers supplied with the NMSO shall include a calibration feature. (M)
4. Refer to Annex B for additional detailed requirements concerning printing requirements. (I)

3.3.7 TOUCH SCREEN MONITORS

1. The Standalone, Desktop Livescan and Cardscan must have touch screen capabilities that will allow the OLU to make onscreen selections by touching specific icons or fields located on the screen instead of using a mouse or keyboard. (M)
2. The Touch Screen Monitor must be a minimum 24-inch Flat Touch Screen Monitor with a maximum resolution of 1920 x 1200 with a 16:10 (8:5) aspect ratio or alternatively a 19-inch Flat Screen Touch Screen Monitor with a maximum resolution of 1280 x 1024 with a 4:3 aspect ratio upon request in the call-up. (M)
3. Refer to Annex B to Appendix A – EFCD Detailed Requirements for additional requirements. (I)

3.3.8 CAMERAS - FACIAL IMAGE CAPTURE REQUIREMENTS

1. The cameras and their associated software must support facial image capture functionality for all Livescans (e.g., Standalone, Desktop and Portable) included in this SOR and its accompanying documents. (M)

2. The cameras and their associated software must use the captured facial image to create a Type-10 record (facial image) that is used to create NPS-NIST-ICD compliant transactions as defined in the NPS-NIST-ICDs. (M)

3. The cameras and their associated software must provide facial image capture capability that will satisfy the following requirements: (M)

    a. the OLU must be able to use a single action (e.g., mouse click on a button) to activate the camera and the camera must automatically activate as required;

    b. the facial image capture device must be a digital camera;

    c. the camera must be connected to a Desktop or Portable Livescan by means of a USB extension no shorter in length than three (3) metres;

    d. the Desktop and Portable Livescan camera must be mounted on fully adjustable telescoping/collapsible tripods, five (5) feet fully extended;

    e. the Desktop and Portable Livescan camera must be powered by either an external or independent power source from a 110 volt power outlet;

    f. the Ruggedized Standalone Livescan Kiosk camera must be powered from within the protective cabinet;

    g. the Ruggedized Standalone Livescan Kiosk solution must include a securely wall-mountable 18% Grey Reflective backdrop appropriately sized for capturing at least the subject's head and shoulders in a vertical image format, and conceal the environment behind the subject;

    h. the Desktop or Portable Livescan system must include a self-supported 18% Grey Reflective backdrop appropriately sized for capturing at least the subject's head and shoulders in a vertical image format, and conceal the environment behind the subject;

    i. the Livescan camera must have:

        i. a facial auto-find feature,

        ii. a visual auto face-centring feature, and

        iii. an auto focus feature;

    j. the Livescan camera must have an automatic white balance feature;

    k. the Livescan camera must have a red-eye reduction feature;

l. the Livescan must present the OLU the option to capture the facial image during the enrolment process;

m. the Livescan must force the OLU to capture the facial image when required by the workflow;

n. the Livescan must present the facial image on screen during the capture process;

o. the Livescan must allow the OLU to capture the facial image by means of a single action (e.g., mouse click on a button, screen touch);

p. the Livescan must allow the OLU to recapture the facial image multiple times;

q. the Livescan must capture and store:

   i. 0 – 1 full face frontal pose for a MAP transaction,

   ii. 0 – 3 facial poses for a CAR-Y or REF transaction
   (i.e., full face frontal pose, left, right or angled profile),

   iii. 0 – 3 facial poses for a CAR-N
   (For local retention on Livescan only or for use on related agency systems – must not form part of NIST Packet) and

   iv. 1 – 3 facial poses for a IMM transaction
   (For local retention on Livescan only or for use on related agency systems – must not form part of NIST Packet);

r. the Livescan must present the OLU with the onscreen view of the last facial image captured;

s. the Livescan application must clearly display onscreen which pose the OLU is capturing;

t. the Livescan must allow the OLU to save a facial image or images;

u. the camera's imaging sensor should only be active during the photo capture step;

v. the Livescan must include the facial image(s) as a Type-10 record(s) as required in NPS-NIST-ICD transactions and also store them in a folder on the Livescan or designated storage media in JPEG format;

w. the Livescan must store the original facial images (i.e. not from the image in the NIST packet) in a configurable folder on the Livescan or designated storage media, with a filename format of [Surname].[DCN].[imagenumber].jpeg, in JPEG format for future recall, export or printing;

x. the Livescan must allow the OLU to send a selected facial image to a printer when captured;

y. the Livescan must allow the recall of a specific transaction by DCN or TCN and present the OLU the option to view the facial images;

z. the Livescan must allow the OLU to send a facial image as a print job by engaging a one step print function or button; and

aa. the Livescan must allow the OLU to export the facial image in JPEG format to an external medium.

4. There should be an auto face-centering indicator over the facial capture for ease of use. (R)

3.3.9 SOFTWARE

1. The Vendor will be responsible for providing licenses and support for all non-GFE software products. The Vendor will also be responsible for upgrades/changes to GFE software as indicated in Section 4.6 GFE Clarification and throughout this SOR and its accompanying documents. The Vendor's proposal must explain how each software product is used by the Vendor's solution to satisfy the requirements stated throughout this SOR and its accompanying documents. (M)

2. COTS software provided as part of the NMSO is expected to be specific to the solution. In other words, the Vendor is not expected to provide any standard Office Automation (OA) products (e.g., e-mail client, word processing, and spreadsheet) as the RCMP/GC/CPMGs currently have negotiated licences for its standard suite of OA products. (I)

3. Additionally, the RCMP/GC/CPMGs has licenses to other software used as part of other operational activities which has been identified throughout this SOR and its accompanying documents (e.g. McAfee client software, WSUS, SCCM). (I)

4. The Vendor must accept that the RCMP/GC/CPMGs may have additional application software that runs on the Livescan/Cardscan (e.g. booking system) and the RCMP/GC/CPMGs will ensure the software will operate without affecting the operation of Livescan/Cardscan. (M)

4. APPROACH FOR APPROVAL OF NMSO DEVICES

4.1 Purpose

1. This section provides an overview of the approach that will be used to approve the NMSO devices after contract award. (I)

2. This section also describes the approval/recertification process for Civil Efficiencies and Charge features that may not be available for the initial approval of the NMSO devices. (I)

4.2 Changes to Certified Devices

1. The Vendor's EFCDs would have been previously certified to ICD 1.7.8 Rev 1.6 with the Vendors OS and configuration. However, the NMSO EFCDs must be approved, and recertified, if necessary, with an RCMP/GC/CPMGs approved OS and configuration. (M)

2. The Vendor must complete all required changes necessary to satisfy all the requirements in this SOR and its accompanying documents that were not satisfied by the Vendor's ICD 1.7.8 Rev 1.6 Certified EFCDs including the Rated requirements identified as met or will be met in the Contractor's proposal. (M)

3. The Vendor must complete all required changes necessary to satisfy all the requirements in this SOR and its accompanying documents for the Vendor's SMTP-SPOI server(s). (M)

4. The Vendor must install their software on the RCMP/GC/CPMGs approved OS on the Vendor's EFCDs and ensure all the requirements in this SOR and its accompanying documents are satisfied. (M)

5. The Vendor must configure the Vendor's EFCDs to support RCMP/GC/CPMGs automatic WSUS updates. The Vendor's EFCDs must satisfy all the requirements in this SOR and its accompanying documents with the RCMP/GC/CPMGs WSUS configuration. (M)

6. The Vendor must configure the Vendor's EFCDs to support the RCMP/GC/CPMGs McAfee ePo or alternative anti-virus software if McAfee is not used. The Vendor's EFCDs must satisfy all the requirements in this SOR and its accompanying documents while receiving ePo, updates, or alternative anti-virus software if McAfee is not used, based on the RCMP/GC/CPMGs configuration. (M)

7. The Vendor must complete the above five (5) items (#2 thru #6), to allow the RCMP recertification/acceptance testing to start, within six (6) months of contract award. (M)

8. The Vendor should complete the above five (5) items (#2 thru #6) as quickly as possible, to allow the RCMP recertification/acceptance testing to start, as soon as possible. (R)

9. If the Vendor's EFCDs do not operate as expected with the RCMP/GC/CPMGs ePo rules, the rules may be adjusted by the RCMP/GC/CPMGs. This will be accomplished by providing a separate set of rules for the EFCDs if required. It is preferred that the Vendor's EFCDs have already been proven to work with ePo and WSUS in an operational environment similar to the RCMP/GC/CPMG. (R)

4.3 Recertification / Acceptance of EFCDs

1. After completing the updates necessary to satisfy all the requirements in this SOR and its accompanying documents, the Vendor's EFCDs will start an recertification/acceptance testing process. This recertification/acceptance testing may be part of a release process. (I)

2. Essentially, the certification process will be redone with as many tests as required by the RCMP to validate that the EFCDs satisfy all the requirements in this SOR and its accompanying documents with all the required changes. The number of tests that are completed will be determined based on how many changes the Vendor completed in order to satisfy the requirements. (I)

3. The Vendor's solution must successfully pass the RCMP re-certification and acceptance testing with all the required changes completed. (M)

4. If the Vendor's solution included the ability to reuse GFE components, this recertification/acceptance testing will also be used to ensure all the requirements in this SOR and its accompanying documents are satisfied with the Vendor's solution implemented on GFE. (I)

5. The Vendor's solution must successfully pass the RCMP re-certification and acceptance testing with all the required changes completed with the reused GFE. (M)

6. It is at the sole discretion of the RCMP/GC/CPMGs what, when, where and how the EFCDs will be tested to determine if they satisfy all the requirements in this SOR and its accompanying documents. This testing will be completed in secure GC facilities based on the data being processed. (I)

7. If the Vendor's EFCD cannot be approved/recertified and successfully pass a DSB Vulnerability Assessment (VA), the EFCD will be considered noncompliant and will not be included on the list of approved NMSO devices. (I)

8. If the Vendor's EFCDs cannot be approved/recertified and successfully pass a DSB Vulnerability Assessment (VA), the Vendor may be considered noncompliant, the contract may be terminated and next most qualified Vendor may be considered for the NMSO. (I)

9. All defects identified by the RCMP through this approval/recertification process must be corrected by the Vendor as quickly as possible using experienced resources. (M)

4.4 Available For NMSO Procurement

1. Once the EFCDs have been approved/recertified by the RCMP, they will be available for procurement or upgrade for all RCMP/GC/CPMGs departments. (I)

4.5 Retested For Civil Efficiencies And Charge Features

1. Once the Civil Efficiencies and Charge features are available in RTID, the EFCDs will be retested with RTID to ensure all features are operating as expected. That is, the configurable parameters will be set to turn on the Civil Efficiencies and Charge features to allow these features to be tested with RTID. This retesting will be completed by RCMP staff to thoroughly test all aspects of these features. (I)
2. Any EFCDs Civil Efficiencies and Charge features that do not satisfy the requirements and are considered defects must be corrected by the Vendor at no additional cost to the RCMP/GC/CPMGs. (M)
3. Once the EFCDs are retested with the Civil Efficiencies and Charge features and approved/recertified by the RCMP, Agencies will be notified that these features can now be turned on in the Production environment. (I)

4.6 GFE Clarifications

1. The following clarifies the separation of responsibilities between the RCMP/GC/CPMGs and the Vendor regarding the GFE. The specific requirements are stated throughout the SOR and its accompanying documents: (I)

    a. GFE workstations:

        i. most GFE workstations are currently configured with Windows 7. The license cost to upgrade these workstations, if required, to Windows 10 would be provided by the RCMP/GC/CPMGs, unless specifically identified by the RCMP/GC/CPMGs within a procurement,

        ii. all components (e.g., flatbed scanners, scanner blocks, Kiosk chassis, etc.) included in the GFE are available for use by the Vendor,

        iii. the hardware maintenance contract for the GFE workstations will be provided by the RCMP/GC/CPMGs, unless specifically identified by the RCMP/GC/CPMGs as part of the NMSO procurement,

        iv. GFE changes that increase the maintenance cost will be specifically identified by the RCMP/GC/CPMGs as part of each NMSO procurement, and

        v. The GC understands that certain components may only operate on Windows 7 or 10; therefore, GC understands that under these conditions the EFCD solution using the GFE components will operate using the compatible Windows OS version or the component will be replaced by the GC;

    b. GFE servers:

        i. the hardware maintenance contract for the GFE servers will be provided by the RCMP/GC/CPMGs, unless specifically identified by the RCMP/GC/CPMGs as part of the NMSO procurement, and

        ii. GFE changes that increase the maintenance cost will be specifically identified by the RCMP/GC/CPMGs as part of the NMSO procurement;

    c. GFE Printers, Scanners and Cameras:

        i. the hardware maintenance contract for the GFE printers, scanners and cameras, as they are configured at the time of contract award, will be provided by the RCMP/GC/CPMGs (i.e., GFE changes that increase the maintenance cost will be the responsibility of the Vendor). Refer to Annex E for GFE details;

d. GFE SAN:

   i. for any Vendor devices (e.g. SMTP-SPOI) that require access to SAN, the NMSO procurement will include whatever details required to support the solution, if allowed by the RCMP/GC/CPMGs;

e. Simple Network Management Protocol (SNMP) reporting:

   i. the RCMP/GC/CPMGs will provide an SNMP reporting system, as required;

f. GFE WSUS and Anti-Virus (ePo):

   i. the RCMP/GC/CPMGs expects to provide WSUS updates to workstations and Windows servers,

   ii. the RCMP/GC/CPMGs expects to provide McAfee antivirus updates including client software on any supported device, and

   iii. the operating system update and AV update requirements that the Vendor must support are identified in this SOR and its accompanying documents; and

g. PC Duo or other Remote Control Application:

   i. the RCMP/GC/CPMGs may provide the licenses for PC Duo, IBM Endpoint Manager (IEM) or other similar product for use with the EFCDs by the Vendor's support staff.

2. All other changes required (e.g., changes to successfully pass a VA, configure for Vendor components, etc.) to support the Vendor's solution and satisfy the requirements stated in the SOR and its accompanying documents must be provided by the Vendor, including, but not limited to at least the following: (M)

   a. all GFE server changes, including operating system upgrades, must be provided by the Vendor, unless specifically identified by the RCMP/GC/CPMGs as part of the NMSO procurement;

   b. all changes to the GFE printers and/or scanners required to support the Vendor's solution and satisfy the requirements stated in the SOR and its accompanying documents must be provided by the Vendor;

   c. the Vendor must provide an SNMP Version 3 agent for any server that is part of their solution;

   d. the RCMP/GC/CPMGs may provide the backup, restore, recovery products; however, the Vendor must have a backup/restore solution for the servers provided through this NMSO procurement;

   e. the Vendor must be able to provide a process to maintain Windows updates and AV for any RCMP/GC/CPMGs that does not have an automated update process;

   f. the Vendor must be able to provide a remote access control method to perform support and maintenance on EFCDs as described throughout the SOR and its accompanying documents, if it is not provided by the RCMP/GC/CPMGs;

3. The Vendor must be able to use GFE procured through alternate RCMP/GC/CPMGs (e.g. workstation NMSO) that have hardware and configuration specifications that meet the requirements in this SOR and its accompanying documents and is comparable in function and form with the with the Vendor's proposed hardware. (M)

5. VENDOR CORPORATE AND MANAGEMENT REQUIREMENTS

5.1 Purpose

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

2. The Vendor must identify at least two (2) previous Livescan/Cardscan NMSOs (or equivalent contractual arrangements) that they have supported that are of a similar size and scope as defined in this SOR and its accompanying documents that includes the supply of at least one hundred (100) users/devices involved in fingerprint processing with at least twenty (25) EFCDs over the life of the contract. (M)

3. The Vendor must have a proven record developing and implementing Livescan and Cardscan devices with at the least five (5) years' experience in the biometric industry. (M)

4. The Vendor should describe its proven ability to support an NMSO of the size and scope as defined in this SOR and its accompanying documents by providing any additional information that support the following requirement: (R)

    a. identify the number of current and/or previous EFCD supply arrangements or contracts supported by specifically identifying up to five (5) clients with requirements similar to the requirements in this SOR and its accompanying documents;

    b. describe the number of years for which the above supply arrangements or contracts were supported;

    c. identify the Vendor's contract value provided in the supply arrangement or contract; and

    d. identify the country for which the supply arrangements or contracts were supported.

5. The Vendor must have sold/supported at least 300 EFCDs to demonstrate their experience and ability to support the requirements stated in the SOR and its accompanying documents. (M)

6. The Vendor must maintain a nationwide maintenance service network, which means that the Vendor must have a sufficient number of resources to meet the response times specified requirements stated in the SOR and its accompanying documents, throughout Canada. (M)

7. The Vendor must have an existing and experienced technical support infrastructure, staffed with personnel trained on the Vendor's devices. (M)

8. The Vendor should describe this nationwide service network and the resources involved to demonstrate how the support and maintenance requirements will be satisfied. (R)

5.2 Planning and Oversight

5.2.1 GENERAL

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

2. The Vendor should provide quality resources and their related EFCD and NMSO experience. (R)

3. All Vendor resources proposed must meet or exceed the following minimum qualifications below and deliver the services required to satisfy the requirements of this Standing Offer: (M)

    a. Project Manager with five (5) years' experience within the last eight (8) years as a project manager and duties that include, but are not limited to"

        i. be responsible for the delivery of all changes required to the Vendor's EFCDs to satisfy the requirements stated throughout the SOR and its accompanying documents,

        ii. act as point of contact between the RCMP and the vendor,

        iii. manage the execution of the task authorizations through development and implementation to ensure the resources are made available and that the requirements of the task authorizations are fully operational within the previously agreed time, cost and performance parameters,

        iv. formulates statement of problems; establishes procedures for the development and implementation of modified task authorization elements and obtains prior RCMP approval,

        v. provide feedback on level of effort, timelines and costs,

        vi. progress reporting on status,

        vii. provides options to problems encountered and recommendations for resolution,

        viii. delivery of new code base, implementation and testing,

        ix. updated design specification documentation, and

        x. analyze the Task Authorizations and perform the above duties as required after the initial updates to satisfy the requirements in the SOR and its accompanying documents;

    b. Systems Engineer with five (5) years' experience within the last eight (8) years as a systems engineer demonstrated experience in designing and integrating workflow modifications within existing systems and duties that include, but are not limited to:

i. be responsible for the engineering changes required to the Vendor's EFCDs to satisfy the requirements stated throughout the SOR and its accompanying documents,

ii. act as the lead engineer for any activity that may or will alter the baseline application code after the initial updates to satisfy the requirements in the SOR and its accompanying documents,

iii. translate business requirements to systems design and specifications,

iv. analyze functional requirements to identify information, procedures and design flows,

v. develop and maintain complex system and modules, programs, sub-systems, system and procedures,

vi. develop technical specifications for systems development, design and implementation,

vii. maintain information coordination between all partners,

viii. lead projects technically through the entire Software Development Life Cycle (SDLC).

ix. deliver production ready enhancements/updates to Vendor products,

x. design and document in detail all affected system components, their interfaces, relationships and operational environment,

xi. document system design, concepts and facilities,

xii. complete system documentation, and

xiii. analyze the Task Authorizations and perform the above duties as required after the initial updates to satisfy the requirements in the SOR and its accompanying documents;

c. Software Engineer with five (5) years' experience within the last eight (8) years as a software engineer with duties that include, but are not limited to:

i. be responsible for interpreting the impact and necessary modifications or enhancements to the baseline application code the software changes require to support to have the Vendor's EFCDs satisfy the requirements stated throughout the SOR and its accompanying documents,

ii. design data structures and files, sub-systems and modules, programs and production monitoring procedures, testing strategies and system,

iii. review the analysis and the programming of other software developers to ensure quality,

iv. perform independent verification and validation of software applications and systems function and performance,

v. prepare the system for production releases and coordinate all changes with impacted partners,

vi. analyze performance and tune systems,

vii. provide guidance and work leadership to other team members.

viii. complete any and all analysis in the vendor's notation that will be used by the software developer to make the necessary application code amendments or enhancements,

ix. develop and document detailed statements of conversion requirements based on client needs and system architectural guidelines,

x. develop and document both high and low-level data mapping requirements and schemas across various corporate systems and databases,

xi. complete system documentation, and

xii. analyze the Task Authorizations and perform the above duties as required after the initial updates to satisfy the requirements in the SOR and its accompanying documents;

d. Software Developer with three (3) years' experience within the last five (5) years with duties that include, but are not limited to:

i. be responsible for the software development changes required to the Vendor's EFCDs to satisfy the requirements stated throughout the SOR and its accompanying documents,

ii. interpreting any associated analysis and implementing any necessary application code changes,

iii. develop and maintain system and modules, programs, sub-systems, and system procedures,

iv. analyze, design and develop classes and their methods, attributes and relationships,

v. design programs, present program design, and write modules and procedures,

vi. provide problem debugging and resolution,

vii. deliver modified application software build with the modifications applied as required to fulfill the requirements,

viii. produce operational systems, including all forms, manuals, programs, input/output sources, procedures and training material,

ix. document program design and quality assurance standards to be used during the implementation phase,

x. complete system documentation, and

xi. interpret the Task Authorizations and perform the above duties as required after the initial updates to satisfy the requirements in the SOR and its accompanying documents;

e. Tester with two (2) years' experience in the last five (5) years with establishing and executing EFCD test plans and procedures to verify customer requirements, regression testing and performance baselines; experience in developing software scripts to conduct testing, and to identify, install, and configure new software and hardware in support of integration testing; with duties that include, but are not limited to:

   i. develop an overall test strategy for the software development changes required to the Vendor's EFCDs to satisfy the requirements stated throughout the SOR and its accompanying documents,

   ii. develop test cases to validate the requirements have been met and ensure the test cases also include regression testing to confirm that existing functionality has not been negatively impacted by any application code modifications or enhancements,

   iii. perform test planning and coordination,

   iv. decide on testing tools, techniques and processes,

   v. develop, manage and monitor test plans for all levels of testing; and

   vi. provide other related test services.

   vii. deliverables will include, but are not limited to:

   viii. provide reports to management on testing status and success,

   ix. maintain and update relevant enhancements in manual or electronic files,

   x. develop standards and processes to follow with regards to system integration, testing and the readying of systems for implementation and rollout,

   xi. provide a fully tested and production ready application, and

   xii. perform all of the above duties for Task Authorizations, as required after the initial updates to satisfy the requirements in the SOR and its accompanying documents;

f. Technical Writer with three (3) years' experience in the last five years as a technical writer with duties that include, but are not limited to:

   i. complete the technical writing for all documentation for the changes required to the Vendor's EFCDs to satisfy the requirements stated throughout the SOR and its accompanying documents,

   ii. work with design team in determining any modifications required to the baselined Detail Design Specification,

   iii. update the Detail Design Specification to incorporate any modifications.

   iv. update user manuals, help text and any other technical documentation,

   v. review documentation standards and existing design specification documentation,

vi. investigate the accuracy of the information collected by making direct use of the material being documented,

vii. prepare or coordinate the preparation of any required illustrations and diagrams,

viii. ensure updated Detail Design Specification accurately reflect any modifications to the baselined specification,

ix. update detail design illustrations or diagrams,

x. update affected help files,

xi. update affected training material, and

xii. perform all of the above duties for Task Authorizations, as required after the initial updates to satisfy the requirements in the SOR and its accompanying documents; and

g. Technician with two (2) years' experience in the last five (5) years with resolving all non-software related technical issues such as hard drive failures, RAM upgrade, Network Interface Card failures, etc. with the Vendor's EFCDs.

5.3 Vendor Organization

5.3.1 VENDOR ORGANIZATIONAL STRUCTURE

1. The Vendor must provide an organizational chart and associated text that describes the organization and how it proposes to address the requirements of this Contract. This description should address at least the following: (M)
    a. the proposed resources and their qualifications:
        i. the roles and responsibilities of each resource; and
        ii. a Curriculum Vitae (CV) for each resource;
    b. the reporting relationship, including the resources reporting relationship to their senior management;
    c. the interface points between the Vendor's resources and RCMP resources that should include an executive sponsor and a Single Point Of Contact; and
    d. the previous experience of the resource supporting Livescan/Cardscan NMSOs that are of the size and scope as defined in this SOR and its accompanying documents.

2. The Vendor should provide sufficient organizational structure information that allows the most effective assessment of the Vendor's ability to support responding to requests and managing the Contract, such as the individuals responsible for managing the contract, the resources and process for delivery of devices, the resources and process for delivery of services and details concerning the provision of warranty and maintenance services. (R)

3. The Vendor should provide resources that already have RCMP/GC/CPMGs security clearances or resources capable of obtaining RCMP/GC/CPMGs security clearances that allow them to satisfy the requirements stated in the SOR and its accompanying documents. This information should include at least a personnel list of all those who will be involved in this NMSO, including their alternates, including name, citizenship, nature of involvement, and any current RCMP and/or PSPC Canadian Industrial Security Directorate (CISD) security clearance status and if the resources do not have a Canadian clearance, identify clearances with other countries. (R)

4. No Vendor resources are allowed to work on the NMSO without prior approval by RCMP/GC/CPMGs and must have an appropriate RCMP/GC/CPMGs clearance based on the resource's responsibilities. (I)

5.3.2 EXECUTIVE SPONSOR

1. The Vendor 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 Vendor, concerning the Contract resulting from this SOR. The executive sponsor is expected to directly resolve any issues relating to this Contract on behalf of the Vendor. The organizational structure should depict the ultimate authority of the executive sponsor. If the executive sponsor is not the ultimate authority, then the executive level that represents the ultimate authority must be identified as well as the types of decisions that are expected to be directed to the ultimate authority. (R)

5.3.3 SINGLE POINT OF CONTACT (SPOC)

1. The Vendor must identify a SPOC that will be assigned to the Contract resulting from this SOR that has the authority and responsibility to directly or indirectly action NMSO procurements, Task Authorizations (TAs) and reporting requests, and perform the tasks associated with this SOR and its accompanying documents. (M)

2. The Vendor’s SPOC and any other proposed resources directly interacting with the RCMP must have good oral and written communication skills. (M)

5.3.4 TECHNOLOGY AND PROCESS

1. The Vendor must describe any tools and processes that they have previously used to perform the tasks required for this Contract. These tools and processes must demonstrate the Vendor's ability to efficiently and effectively support the requirements defined in this SOR and its accompanying documents. (M)

2. The Vendor must, at a minimum, describe their delivery, installation, integration, support and maintenance processes and previous experience to demonstrate the Vendor's ability to satisfy the requirements stated throughout this SOR and its accompanying documents for Livescans and Cardscans. (M)

3. The Vendor should describe any tools and processes that they will use to perform the tasks required for this Contract in the most efficient and effective manner. (R)

4. The Vendor should provide their Delivery, Installation, and Integration Plan describing: (R)

    a. how they will ship, upon receiving a call-up, the device hardware, software, and documentation;

    b. a complete description on how change orders will be processed, approved, and implemented;

    c. the facility and layout requirements for the use of the devices including at least the space, power, lighting requirements and integration into the RCMP/GC/CPMGs architecture;

    d. the configuration process that allows the device to be setup with the Types Of Transactions (TOTs) and configuration required for the Agency procuring the devices; and

    e. the NMSO reporting process that ensures the NMSO reporting requirements stated throughout this SOR and its accompanying documents are satisfied.

5. The Vendor should describe the setup and installation process for the EFCDs. This description should include a clear indication of how easily the Agency's IT support staff can follow the installation guide to complete the installation, configuration and setup of the EFCD. (R)

6. The Vendor should describe their configuration management control system that ensures the integrity of the device's software/configuration version to ensure all devices procured with a specific set of features is consistently provided the requesting Agencies throughout the life of the NMSO. (R)

5.3.5 DELIVERY AND INSTALLATION

1. The Vendor must agree to supply, deliver, configure, install (if required by a Call-up), integrate and implement (if required by the Call-up), provide warranty, maintenance software support services and documentation for the EFCD(s) and other products ordered under this NMSO (as specified in the Call-up), to the Identified User, according to the prices, terms and conditions in this NMSO. Products must be delivered on an "as and when requested" basis to the location(s) specified in the Call-up, which may be locations anywhere in Canada when the Call-up is made in accordance with this NMSO. (M)

2. Each product and its supply, delivery, configuration, installation (if required by a Call-up), integration and implementation (if required by the Call-up) including the warranty, maintenance, software support services and associated documentation (as specified in the Call-up) is subject to inspection and acceptance by the Identified User. If the product(s) do not correspond to the System(s) (including configuration), or Component(s) offered under the NMSO or otherwise specified in the Call-up, or if the Products do not meet the Technical Specifications of the Call-up, the Vendor will be in default of this NMSO and Canada may reject the product(s) or require that they be corrected at the sole expense of the Vendor before accepting them. No payment for any product is due under the NMSO unless the product is accepted. No restocking fees or other charges will apply to products that are not accepted. (M)

3. If any product fails to perform in accordance with the Technical Specifications and functional descriptions contained or referenced in the Call-up and requires remedial hardware maintenance service three (3) or more times during the Hardware Maintenance Period, the Vendor must, if requested by the Identified User, replace the product at no cost with another item meeting the specifications of the product. The replacement product must be delivered no later than 15 calendar days after the request is received. The Vendor must restore the system to full operation with the replacement product at no charge. (M)

4. The Vendor must provide the following as part of delivering the product(s): (M)

    a. coordinate delivery schedules to the Call-up site locations within Canada with each call-up;

    b. accepts and agrees that the sites will be specific to a point of destination provided in a call-up;

    c. perform and pay for, as part of the Standing Offer, all the following shipment services to include, at a minimum:

        i. package all hardware and any related software,

        ii. provide any associated commercial documentation,

        iii. identify and contract for any required broker services,

        iv. prepare and submit any appropriate Canadian and US Customs forms,

        v. insure all shipped goods, for full value, either with the shipper or self-insure them, as per their corporate policy,

vi. ship the material with a bill of lading that corresponds to the shipping container, serial number, and BOM item number for use by the Call-up Agency at the point of destination identifying the receipt of all shipped material, and

vii. provide a copy of the Bill of Lading to Call-up Agency point of contact at the time of the shipment(s) through an agreed to method (e.g. fax, email);

d. deliver all hardware, software, peripherals and documents to point of destination;

e. acquire and pay for, as part of the Standing Offer, all appropriate end user license agreements; and

f. provide the client with End User License Agreements for all commercial and shareware software products acquired for use with the procured devices.

5. The Vendor must provide the following as part of the delivery and integration of the product(s): (M)

a. prior to equipment shipment, provide a Delivery and Integration Plan to the Call-up agency with the sequence of installation/integration steps for the equipment including site configuration requirements in terms of space, power and network connections.

b. unpack and set-up the equipment at the delivery location on a schedule that is approved by the client at point of destination.

c. be responsible for the removal of any packaging material originating from the delivered hardware or any of its components to a local site as directed by the client.

d. load and initialize all new application software and Online Help files.

e. support the Call-up agency with RCMP Agency Certification testing and migration to the RCMP production environment.

f. formally inform the RCMP Biometric Business Solutions Section Project Manager in writing of any device or technical issues identified during Agency Certification Testing and their approach to resolve the issues and how other deployed devices will be updated.

6. During the period of this Standing Offer or Warranty or Extended Maintenance, hardware may reach end-of-life and need to be replaced with new hardware. (I)

7. The Vendor must provide the following regarding product substitution: (M)

a. advise the RCMP of replacement hardware that differs in make and model from the original hardware delivered;

b. provide the RCMP with the make and model of the replacement hardware;

c. demonstrate, to the satisfaction of the RCMP, that:

i. the replacement hardware will work seamlessly with their application software with no loss of functionality or any conflicts with the application interface and operating system, and

ii. the replacement hardware in combination with the software remains compliant to the NPS-NIST-ICD 1.7.8 Rev 1.6 Vendor Certification requirements;

d. provide the RCMP with the means to test the new hardware at the RCMP Headquarters, Ottawa, Ontario;

e. address and correct any issues or conflicts identified during RCMP testing; and

f. not deploy new replacement hardware until approved and directed by the RCMP.

6. OVERALL DELIVERABLES PLAN AND SCHEDULE

6.1 Overview

1. This section identifies the Vendor deliverables and describes the content of the deliverables that must be completed as part of this SOR. (M)

2. Expected RCMP deliverables are also listed to allow the Vendor to be aware of these deliverables and ensure they are included in the master schedule with any required dependencies. (I)

3. Any additional deliverables that the Vendor considers important for the successful completion of this SOR must be identified by the Vendor and indicate any RCMP activity related to the additional deliverables. (M)

4. Any additional deliverables that the Vendor requires from the RCMP must be identified. RCMP must approve any changes to the list of deliverables identified in Subsection 6.2 below. (M)

6.2 Contract Deliverables Requirements List (CDRL) Scheduling of Deliverables

1. The following table, Table 6-1: Schedule of Deliverables, identifies the deliverables, responsibility for completion, initial delivery date, revision time period (in business days) and final deliverable dates. (I)

2. The time estimates, identified in Table 6-1, are preferred by the RCMP. (R)

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

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

Table 6-1: Schedule of Deliverables

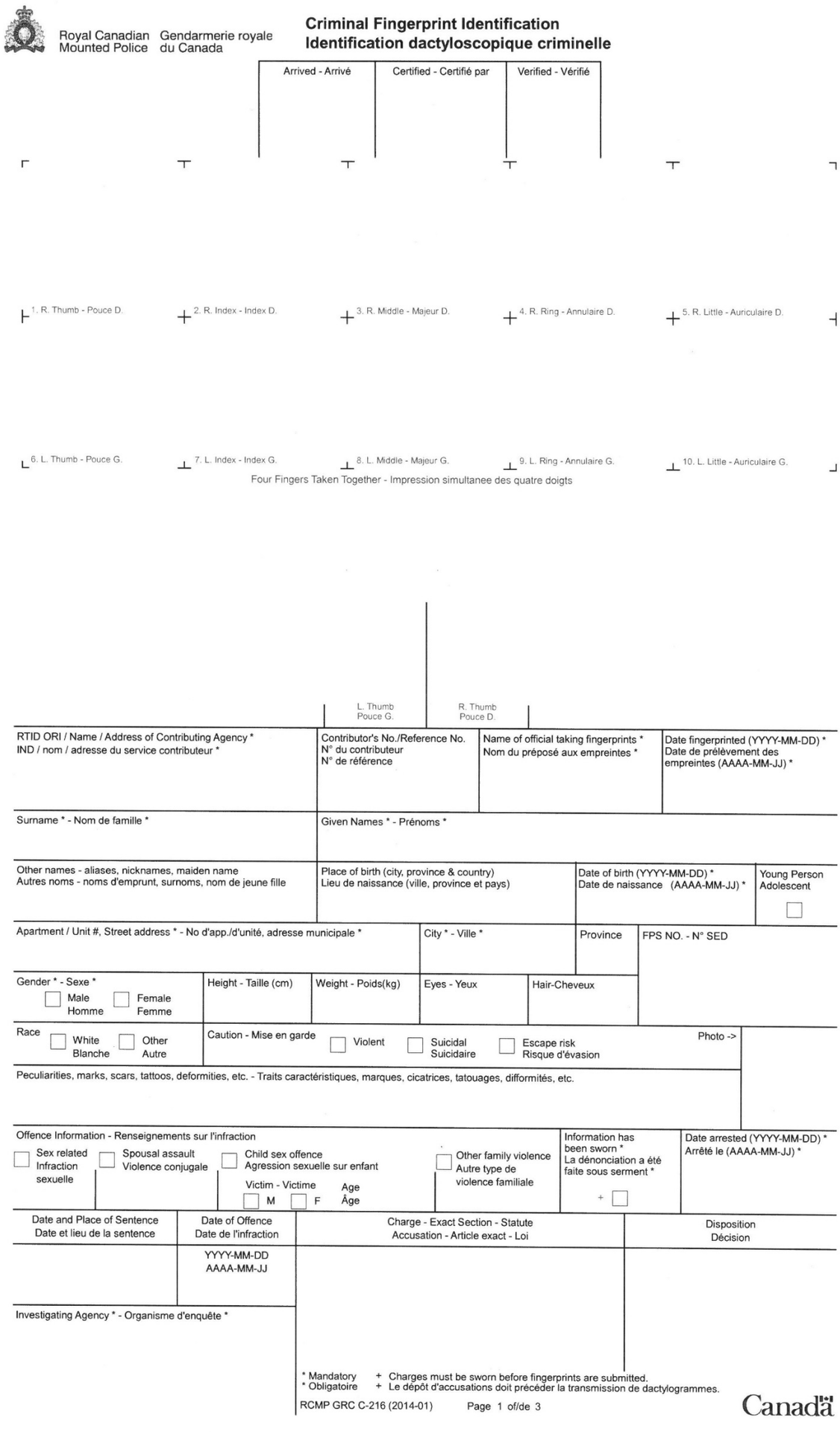
NO.	DESCRIPTION	DID NO.	RESPONSIBLE	INITIAL DELIVERY DATE	RCMP/ GC/ CPMGs REVIEW	UPDATED	FINAL DELIVERY DATE
	PROJECT MANAGEMENT						
1.	Master Contract Schedule (MCS)	N/A	RCMP with Vendor input	Ten (10) days after Contract Award (CA)	5 days	After Vendor review and agreement	Ten (10) days after review and agreement
2.	Requirements Traceability Matrix (RTM) provided in RFP and completed by the Vendor	N/A	the Vendor	RTM only with proposal, for RCMP use, to validate compliance to RFSO requirements	N/A	To include all Contractor agreed to Rated to become full list of Mandatory requirements	Fifteen (15) days after CA
3.	System Design Documentation (SDD)	N/A	the Vendor	With proposal, for RCMP use, to validate compliance to RFSO requirements	N/A	N/A	N/A
4.	Project Documentation • Systems Engineering Management Plan; • Quality Assurance Plan; • Requirements Management Plan; • Configuration Management Plan; • Risk Management Plan; • Problem Resolution Plan • Document Management; and • Sub-Contractor Management Plan.	N/A	the Vendor	With proposal, for RCMP use, to validate compliance to RFSO requirements	N/A	N/A	N/A

Table 6-1: Schedule of Deliverables

NO.	DESCRIPTION	DID NO.	RESPONSIBLE	INITIAL DELIVERY DATE	RCMP/ GC/ CPMGs REVIEW	UPDATED	FINAL DELIVERY DATE
5.	RCMP Certification Letters and sample C-216 forms generated from each certified device.	N/A	the Vendor	With proposal, for RCMP use, to validate compliance to RFSO requirements	N/A	N/A	N/A
6.	CV for proposed resources, references and any other documentation to support all rated criteria	N/A	the Vendor	With proposal, for RCMP use, to validate compliance to RFSO requirements	N/A	N/A	N/A
7.	Training Plan	N/A	the Vendor	With proposal, for RCMP use, to validate compliance to RFSO requirements	5 days	Updated by the Vendor based on RCMP comments	RCMP final approval required
8.	EFCD and SMTP-SPOI User and Admin manuals and training guide(s)	N/A	the Vendor	With proposal, for RCMP use, to validate compliance to RFSO requirements and for use in Benchmark testing, if required.	10 days	Updated by the Vendor based on the changes required to support the RFSO requirements and included with the purchase of devices as required	Depends on the changes required to support the RFSO requirements and on specific NMSO procurements RCMP final approval of updated manuals / guides required
9.	Approved/Recertified EFCDs satisfying NMSO requirements.	N/A	the Vendor	Start within six (6) months following the NMSO contract signing	TBD	Based on agreed to schedule. Deliverable time starts once RTM is agreed to.	RCMP Approval and/or new Certification Letter, if required, implicitly the final delivery
ALL OTHER DELIVERABLES							
10.	Delivery of Bill Of Materials (BOM)	N/A	the Vendor	TBD	TBD	Depends on NMSO procurement	Depends on NMSO procurement

ATTACHMENT A-1 – FINGERPRINT FORMS

Criminal Fingerprint Identification C-216 Form



Royal Canadian Mounted Police / Gendarmerie royale du Canada

Criminal Fingerprint Identification
Identification dactyloscopique criminelle

Arrived - Arrivé	Certified - Certifié par	Verified - Vérifié

1. R. Thumb - Pouce D. | 2. R. Index - Index D. | 3. R. Middle - Majeur D. | 4. R. Ring - Annulaire D. | 5. R. Little - Auriculaire D.

6. L. Thumb - Pouce G. | 7. L. Index - Index G. | 8. L. Middle - Majeur G. | 9. L. Ring - Annulaire G. | 10. L. Little - Auriculaire G.

Four Fingers Taken Together - Impression simultanee des quatre doigts

L. Thumb / Pouce G. | R. Thumb / Pouce D.

RTID ORI / Name / Address of Contributing Agency * / IND / nom / adresse du service contributeur *	Contributor's No./Reference No. / N° du contributeur / N° de référence	Name of official taking fingerprints * / Nom du préposé aux empreintes *	Date fingerprinted (YYYY-MM-DD) * / Date de prélèvement des empreintes (AAAA-MM-JJ) *

Surname * - Nom de famille *	Given Names * - Prénoms *

Other names - aliases, nicknames, maiden name / Autres noms - noms d'emprunt, surnoms, nom de jeune fille	Place of birth (city, province & country) / Lieu de naissance (ville, province et pays)	Date of birth (YYYY-MM-DD) * / Date de naissance (AAAA-MM-JJ) *	Young Person / Adolescent ☐

Apartment / Unit #, Street address * - No d'app./d'unité, adresse municipale *	City * - Ville *	Province	FPS NO. - N° SED

Gender * - Sexe * ☐ Male / Homme ☐ Female / Femme	Height - Taille (cm)	Weight - Poids(kg)	Eyes - Yeux	Hair-Cheveux

Race ☐ White / Blanche ☐ Other / Autre

Caution - Mise en garde ☐ Violent ☐ Suicidal / Suicidaire ☐ Escape risk / Risque d'évasion

Photo ->

Peculiarities, marks, scars, tattoos, deformities, etc. - Traits caractéristiques, marques, cicatrices, tatouages, difformités, etc.

Offence Information - Renseignements sur l'infraction

☐ Sex related / Infraction sexuelle ☐ Spousal assault / Violence conjugale ☐ Child sex offence / Agression sexuelle sur enfant

Victim - Victime ☐ M ☐ F Age / Âge

☐ Other family violence / Autre type de violence familiale

Information has been sworn * / La dénonciation a été faite sous serment * + ☐

Date arrested (YYYY-MM-DD) * / Arrêté le (AAAA-MM-JJ) *

Date and Place of Sentence / Date et lieu de la sentence	Date of Offence / Date de l'infraction	Charge - Exact Section - Statute / Accusation - Article exact - Loi	Disposition / Décision
	YYYY-MM-DD / AAAA-MM-JJ		

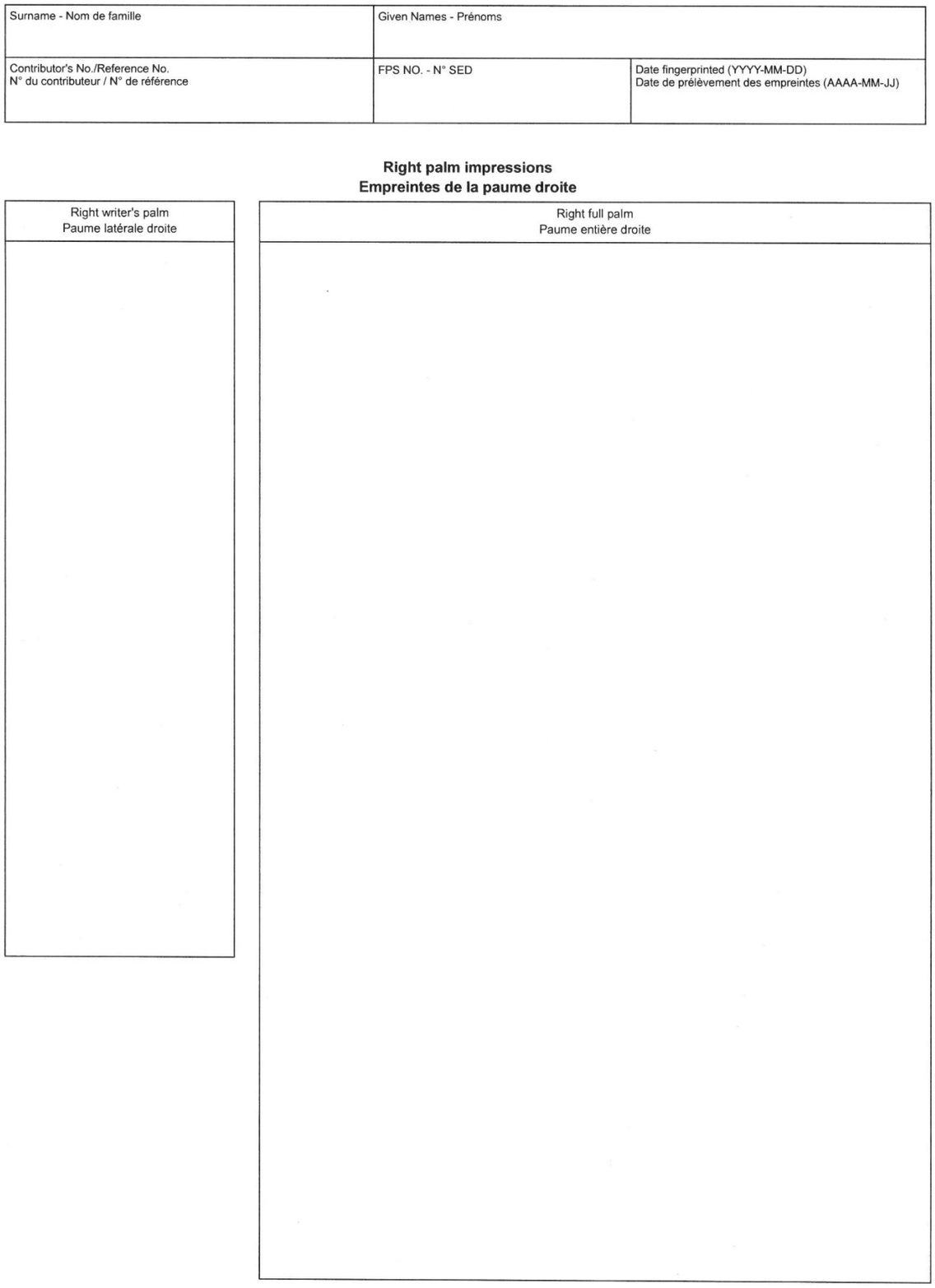
Investigating Agency * - Organisme d'enquête *

* Mandatory / * Obligatoire + Charges must be sworn before fingerprints are submitted. / + Le dépôt d'accusations doit précéder la transmission de dactylogrammes.

RCMP GRC C-216 (2014-01) Page 1 of/de 3

Canada

Figure A-1: Example of C-216 Form, Page 1 of 3



Surname - Nom de famille	Given Names - Prénoms	
Contributor's No./Reference No. N° du contributeur / N° de référence	FPS NO. - N° SED	Date fingerprinted (YYYY-MM-DD) Date de prélèvement des empreintes (AAAA-MM-JJ)

Right palm impressions
Empreintes de la paume droite

Right writer's palm Paume latérale droite	Right full palm Paume entière droite

RCMP GRC C-216 (2014-01) Page 2 of/de 3

Figure A-2: Example of C-216 Form, Page 2 of 3

Surname - Nom de famille	Given Names - Prénoms	
Contributor's No./Reference No. N° du contributeur / N° de référence	FPS NO. - N° SED	Date fingerprinted (YYYY-MM-DD) Date de prélèvement des empreintes (AAAA-MM-JJ)

Left palm impressions
Empreintes de la paume gauche

Left writer's palm Paume latérale gauche	Left full palm Paume entière gauche

RCMP GRC C-216 (2014-01)

Page 3 of/de 3

Figure A-3: Example of C-216 Form, Page 3 of 3

Civil Fingerprint Identification C-216C Form

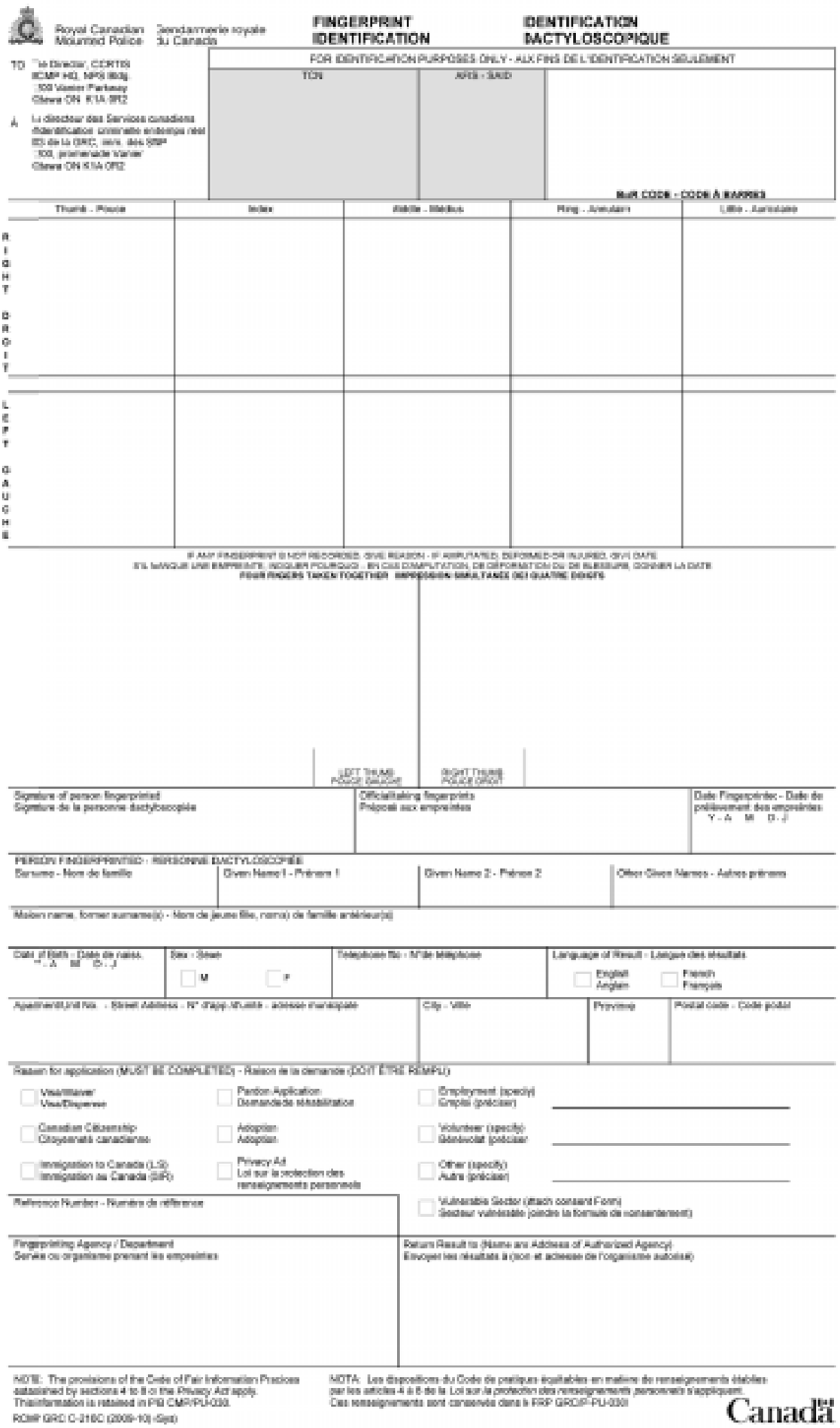


Figure A-4: Example of C-216C Form

Refugee Fingerprint Identification C-216R Form

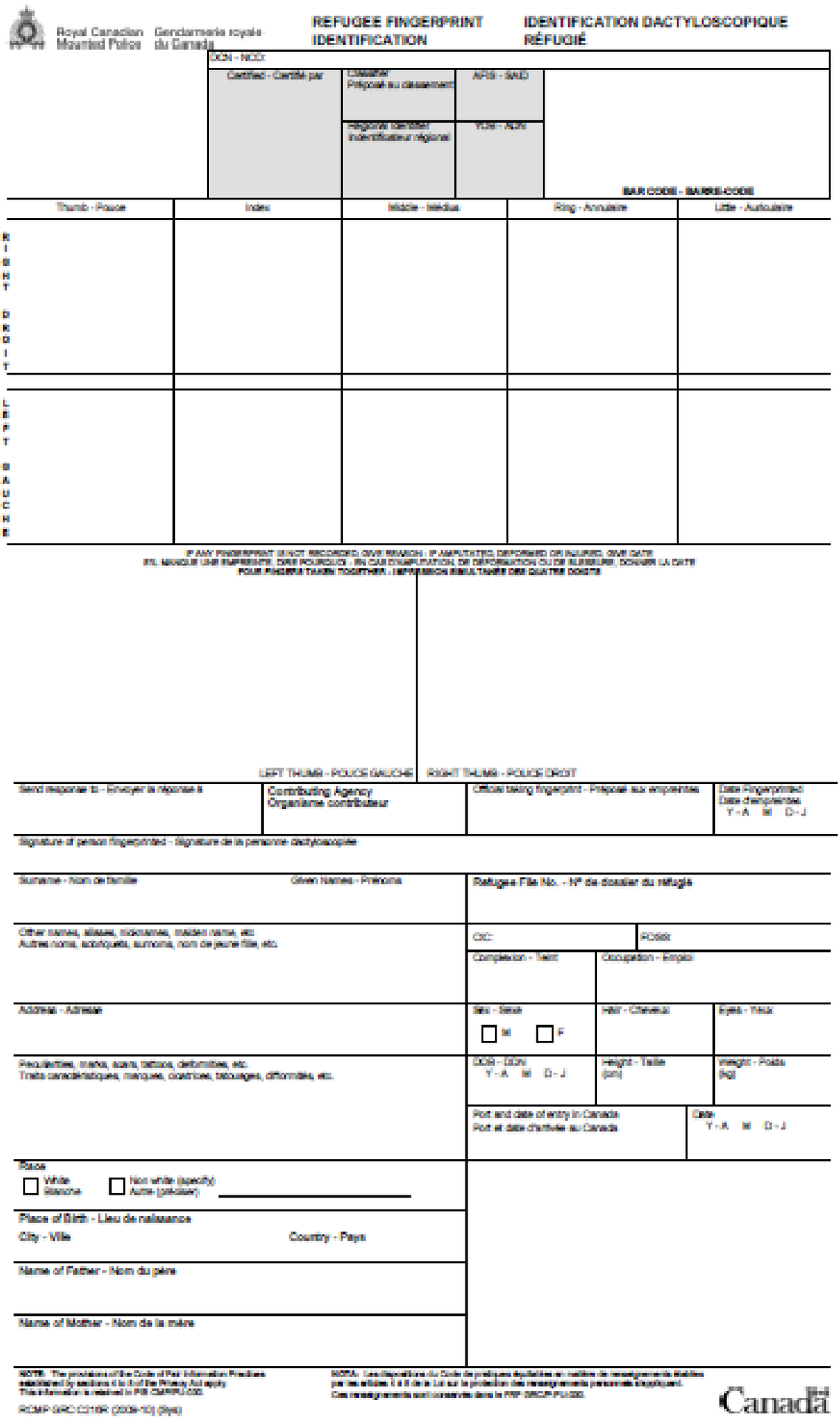


Figure A-5: Example of C-216R Form

Civil Fingerprint Identification Flats C-216C IDFLATS Form

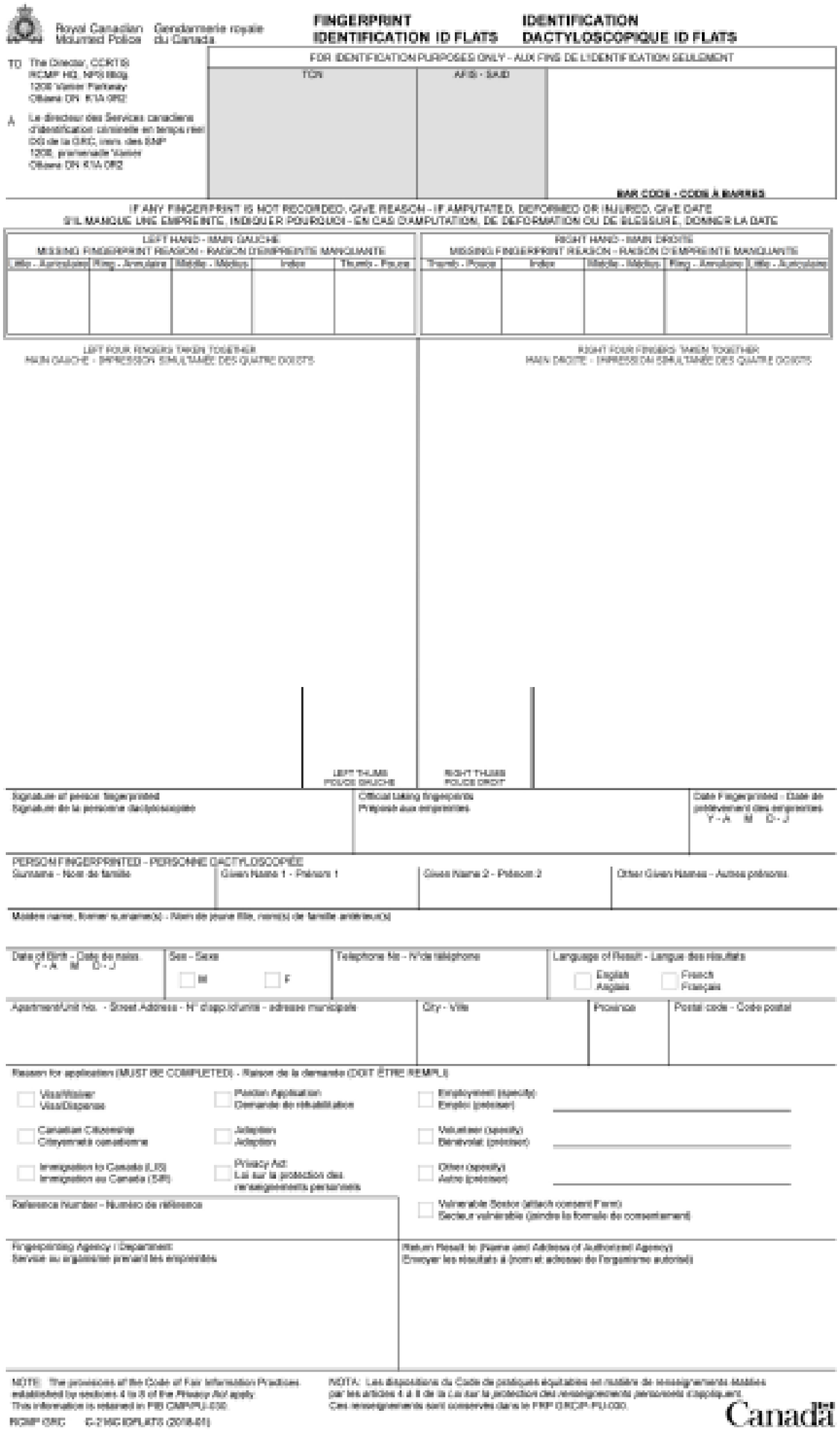


Figure A-6: Example of C-216C IDFLATS Form

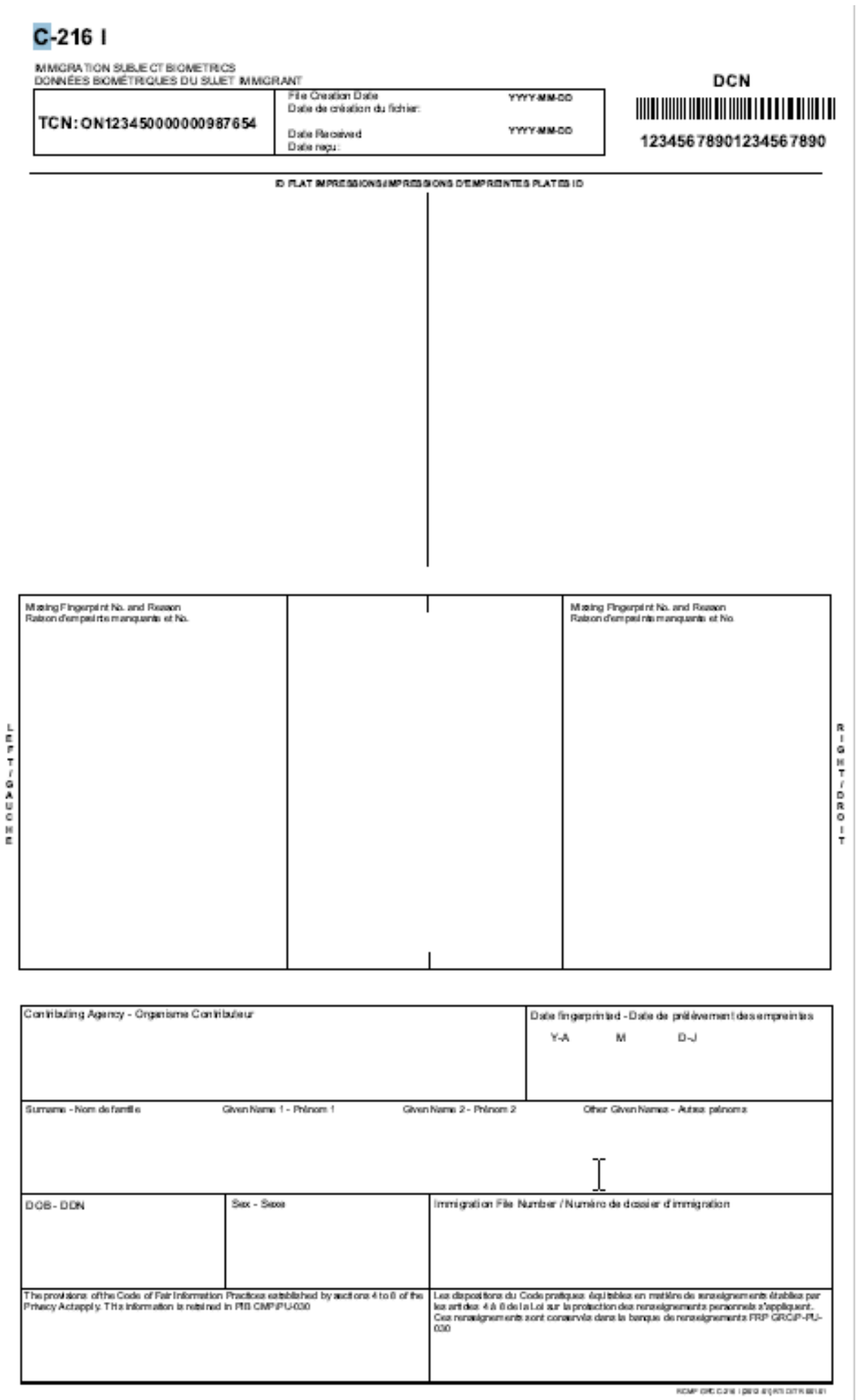


Figure A-7: Example of C-216I IMM IDFLATS Form

ATTACHMENT A-2 – 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 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 Vendor 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 Vendor will commit to completing the deliverables according to this schedule. Any required changes or additions for inclusion in the baseline version of the MCS must be approved by the RCMP Technical Authority.

4. PREPARATION INSTRUCTIONS

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

4.2 Format Requirements. The schedule portion of the MCS shall be presented in Bar (Gantt) chart format. The activities depicted in the chart shall be based on a planned sequence of events with the time estimates, start and end dates for all events precisely calculated. 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 SOR. 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 SOR using the Work Breakdown Structure (WBS) technique. For each element of the WBS, the Vendor 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 SOR, including subordinate shipping, installation and site acceptance schedules as applicable;

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

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

e. The MCS shall identify, as required, the schedule for all deliverables, Project Review Meetings (PRMs), Vendor demonstrations, on-site tests and inspections, installation, acceptance and approval/recertification, as appropriate;

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

g. The RCMP will baseline the final version of the MCS once agreed to with the Vendor 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 Vendor 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 Vendor for the reporting period. Subject of discussion shall include progress to-date against the baseline plan, upcoming deliverables, Vendor 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 offices located at 1200 Vanier Parkway in Ottawa.

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

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

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

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

ii. provide all administrative support;

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

iv. the Vendor must ensure that their qualified Vendor 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

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

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 Vendor to provide representation at ad hoc meetings. These meetings are intended to address matters of a serious nature that cannot reasonably be delayed until the next scheduled formal progress review meeting.

4.3 Agenda and Minutes of Meetings

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

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

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

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

ATTACHMENT A-3 – LIST OF DEFINITIONS

The purpose of this attachment is to define the terminology used within this SOR and its accompanying documents.

Table A-1: Table of Terms and Acronyms

TERM / ACRONYM	DEFINITION
ACKT	Acknowledgement Transaction
Adobe	Adobe Systems Incorporated
AFIS	Automated Fingerprint Identification System
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
AKA	Also Known As
ANSI	American National Standards Institute
ATS	Anonymous Ten Print Search (transaction)
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 SOR and its accompanying documents
AV	Anti-Virus
Biographic Data	Alphabetical and numerical type data contained within a submission. Examples include: Name, Date Of Birth (DOB), and Sex
Biometric Data	Examples are fingerprint images and a facial photograph
CA	Contract Award
CAR-N or CARN	Criminal (Ten Print submission) Answer Retained – No (i.e., information and fingerprint images associated with this submission will not be kept)
CAR-Y or CARY	Criminal (Ten Print submission) Answer Retained – Yes (i.e., information and fingerprint images associated with this submission will be retained)
CBSA	Canada Border Services Agency
CCRTIS	Canadian Criminal Real Time Identification Services
CDRL	Contract Deliverables Requirement List
CISD	Canadian Industrial Security Directorate
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 or display that can be turned on or off; or a variable that affects the operation of the device (e.g. retention period for files, authorized TOTs, functionality specific to a specific function or department/agency, etc.
Contributor	An authorized agency that submits requests for service to CCRTIS. Examples of requests for service include Criminal Retain (CAR-Y), Criminal Inquiry (CAR-N), Civil (MAP), Refugee (REF), and Immigration (IMM) submissions
COTS	Commercial Off-The-Shelf

Table A-1: Table of Terms and Acronyms

TERM / ACRONYM	DEFINITION
CPIC	Canadian Police Information Centre
CPIC (Query)	A Canadian Police Information Centre (CPIC) query retrieve criminal record related data from CPIC
CPMGs	Canadian Provincial/Municipal Governments/Territories
CPSIC	Canadian Police Services Information Centre
CPU	Central Processing Unit
CR	Change Request
CSA	Canadian Standards Association
CV	Curriculum Vitae
DAT	Data files for AV scanning software
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
DCN	Document Control Number
DID	Data Item Description
DMS	Digital Mugshot System
DNA	Deoxyribonucleic Acid
DOB	Date of Birth
DR	Disaster Recovery
DSB	Departmental Security Branch
EBTS	Electronic Biometric Transmission Specification (The FBI's implementation of the ANSI/NIST Standard for the Interchange of Fingerprint Images. i.e., the updated EFTS will be renamed EBTS)
EC	European Council
EFCD	Electronic Fingerprint Capture Device(s)
ePo	(McAfee AV) ePolicy Orchestrator
ERRT	Error (Ten Print) Response Transaction
EST	Eastern Standard Time
FAT	Factory Acceptance Testing
FBI	Federal Bureau of Investigation
Fingerprint Biometric Data	This term refers to fingerprint images contained within a submission
FIS	Forensic Identification Services

Table A-1: Table of Terms and Acronyms

TERM / ACRONYM	DEFINITION
GC	Government of Canada
GCMS	Global Case Management System
GFE	Government Furnished Equipment
HA	High Availability
HQ	Headquarters
HW	Hardware
IAFIS	Integrated Automated Fingerprint Identification System (FBI)
ICAO	International Civil Aviation Organization (a United Nations specialised agency)
ICD	Interface Control Document
ID	Identifier
IDFLATS	Identification Flats (a 4-finger and 2-thumb flat impressions)
IEC	Immigration External Contributor
IID	Immigration Identification (file number) The Immigration Identification File Number is the unique key generated by the RCMP under which Immigration data is stored within the RCMP. An IID Number, once purged, will never be reused
IIS	Immigration Information Sharing (Specifically the Canada-US Immigration Information Sharing project)
IMM	Immigration Enrolment Transaction
IP	Internet Protocol
IQS	Image Quality Specification
IRCC	Immigration, Refugee and Citizenship Canada (formerly Citizenship and Immigration Canada – CIC)
ISO	International Standards Organization
IT	Information Technology
ITL	Information Technology Laboratory (National Institute of Standards and Technology – US)

Table A-1: Table of Terms and Acronyms

TERM / ACRONYM	DEFINITION
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
Layer 3	In the seven-layer OSI model of computer networking, the network layer is Layer 3. Layer 3 is responsible for packet forwarding including routing through intermediate routers
LB	Load Balancing
LOI	Letter Of Interest
MAP	Miscellaneous Applicant Civil
MCS	Master Contract Schedule
MS	Microsoft Corporation
NIST	National Institute of Standards and Technology
NMSO	National Master Standing Offer
NNS	National Police Services – National Institute of Standards and Technology (NPS-NIST) Server (RCMP – Transaction and workflow manager for RTID)
NPS	National Police Service
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
NTP	Network Time Protocol
NTWG	New Technologies Working Group (from the UN specialized agency International Civil Aviation Organization (ICAO))
OA	Office Automation
OLA	Operational Livescan Administrator
OLU	Operational Livescan User
ON	Ontario
OPS	Operational Support
ORI	Originator ORI (CPIC unique identified)
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
OS	Operating System
OSI	The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols
OSPF	Open Shortest Path First
OSR	Operational Statistics and Reporting (code)

Table A-1: Table of Terms and Acronyms

TERM / ACRONYM	DEFINITION
PC	Personal Computer
PC Duo	Application by Vector Networks for PC to PC remote control and remote access over LAN/WAN and internet connections
PDF	Portable Document Format (Adobe Systems Incorporated's open standard for electronic document exchange)
POE	Port of Entry
POP	Post Office Protocol (e.g., POP3)
PP	Palm Print
PR	Primary
PROD	Production (environment)
PS	Police Service
PSPC	Public Services and Procurement Canada (replaces PWGSC)
QA	Quality Assurance
RCMP	Royal Canadian Mounted Police
RDIMS	Records, Documents and Information Management System
REF	Refugee Enrolment (Ten Print – submission type prepared by CBSA/IRCC/RCMP when enrolling a Refugee subject in the RTID system)
RFI	Request for Information
RFP	Request for Proposal
RFSO	Request for Standing Offer
RMS	Records Management System
RTID	Real Time Identification (system)
RTM	Requirements Traceability Matrix
RVD	Request for Volume Discount
SAN	Storage Area Network
SCCM	System Center Configuration Manager (Microsoft Corporation)
SDD	System Design Documentation
SDPPM	Systems Delivery and Project Portfolio Management
SE	System Engineering
SLA	Service Level Agreement
SME	Subject Matter Expert
SMTP	Simple Mail Transfer Protocol

Table A-1: Table of Terms and Acronyms

TERM / ACRONYM	DEFINITION
SNMP	Simple Network Management Protocol
SOR	Statement of Requirements (Work)
SPOC	Single Point of Contact
SPOI	Single Point of Interface
SQL	Structured Query Language
SRE	Search Response
SRL	Search Response Latent
SRLI	Search Response Latent Internal
SSC	Shared Services Canada
SSL	Secure Sockets Layer (authentication, encryption technology and protocol)
Subject	An identified individual with a unique Subject Id (retained) or an incoming submission with unique set of prints (non-retained)
Subject File	This term refers to a specific file associated with a unique Subject ID
Submission	A request for service initiated by an external contributor to add, retrieve, amend, remove, or search for information held in the RCMP National Fingerprint Repository. A submission may contain one or more transactions. For example, an Enrolment contains the following transactions: • an IMM; • if applicable an Error Response Transaction (ERRT); • an Acknowledgement Transaction (ACKT); and • a Search Response (SRE).
Submission Data	This term refers to the data created as a result of processing each submission. Examples include; Activity Log Entries, Status Histories and Internal Transactions to RTID AFIS as well as other Subsystems, etc.
SW	Software
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
TA	Task Authorization
TBD	To Be Determined
TCN	Transaction Control Number (record layout field name or tag)
TOT	Type of Transaction
TP	Ten Print
TPF	Ten Print File
TR	Temporary Resident

Table A-1: Table of Terms and Acronyms

TERM / ACRONYM	DEFINITION
Transaction	This terms refers to a defined interaction within a submission. An exchange of information with the system or a subsystem
TRB	Temporary Resident Biometrics (a.k.a. Immigration)
TT	Transaction Time
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 one (1) to three (3) of the following images: Right Four (4) Fingers; and/or Left Four (4) Fingers; and/or Two (2) Thumbs.
UI	User Interface
ULC	Underwriters Laboratories of Canada
ULF	Unsolved Latent File
UPS	Uninterruptible Power Supply
US	United States (of America)
USB	universal serial bus
User(s)	The term User or Users refers to CCRTIS Authorized User(s) that have been provided access to the function or User Interface (UI) referred to in these requirements
VA	Vulnerability Assessments
Verification	Comparing a candidate fingerprint / palm print to a search fingerprint / palm print
Verification Repository	This term refers to the IMM biometric fingerprint and encoding (minutiae) created and retained for Verification (VSS) purposes. It also includes the image data and biographical information
Verification Subsystem (VSS)	The term Verification Subsystem is defined as all the components required to fully support all Verification Subsystem requirements
VSP	Virtual Storage Platform
VSS	Verification Subsystem
WI	Work Item (RCMP Software/Solution Incident Report)
WSQ	Wavelets Scalar Quantization (a compression algorithm that uses wavelet technology)
WSUS	Windows Server Update Services