RCMP·GRC
ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

Canadian Criminal Real Time Identification Services

Real Time Identification (RTID):
Introduction for Agencies

RTID Introduction for Agencies

RCMP GRC

Date:	2012-02-07
Status:	Final
Version:	16.0
Classification:	Unclassified
Owner:	CCRTIS Policy Centre
RDIMS:	19085

RECORD OF AMENDMENTS

Version No.	Date	Comments
1.8 (Final)	2006-10-25	Updates from CCC Technical Writer.
2.0 (Draft)	2008-07-09	Disclaimer updated (pg 3). Section 1 updated with current material. Sections 2-3 updated to reflect current certification process.
2.1 (Draft)	2008-12-31	Removed testing component from agency certification.
2.2 (Draft)	2010-12-30	Removed Work Order and Telenet Test. Added Agency Profile update requirements. Changed Workflow Manager to RTID system. Added details under Section 2.3 Considerations.
3.0 (Draft)	2011-01-24	Removed Agency Application Form (Appendix A). Updated Cover Page to CCRTIS. Updated Document Origin and Approval Record to CCRTIS. Added SLA caveat *** Section 1.10.

DOCUMENT ORIGIN AND APPROVAL RECORD

Approvals	Position (Actual signatures are found on a formal deliverable checklist)
Acceptor	CCRTIS Director General
Acceptor	OIC, CCRTIS Operational Support & Client Services
Acceptor	OIC, CCRTIS Biometric Business Solutions
Policy Centre	CCRTIS Operational Support & Client Services

DISCLAIMER

The purpose of this document is to provide contributing agencies with an overview of the National Police Services – National Institute of Standards and Technology (NPS-NIST) Agency Certification Process.

While the Royal Canadian Mounted Police (RCMP) has provided guidelines for preparing agencies for RTID, the RCMP makes no claims as to the completeness and accuracy of the documentation herein. It is the user of this information who is ultimately responsible for the adaptation and integration of changes into existing systems and the ensuing results. The RCMP, Forensic Science and Identification Services (FS&IS), and the Canadian Criminal Real Time Identification Services (CCRTIS) disclaim any responsibility, liability, costs, loss of efficiencies or other economic loss whether direct or consequential, flowing from any use made by the user of this information and other materials provided herein.

The RCMP makes no warranties, express or implied, and specifically disclaims any implied warranty of merchantability or fitness for a particular purpose. The RCMP will not be responsible for any errors or omissions which may have occurred in the drafting of this information and expressly disclaim liability whether under contract or in negligence to any user of the work whether a direct user, any person who may borrow or use it or to any client of such a person.

In taking possession of this document, the user agrees to not release this document to a third party without the expressed written permission of the RCMP. The user of this document acknowledges, agrees and accepts the foregoing and releases, agrees to indemnify and hold harmless the RCMP, FS&IS and CCRTIS.

INDEX

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide contributing agencies with an overview of the Real Time Identification (RTID) Project, and the National Police Services – National Institute of Standards and Technology (NPS-NIST) Agency Certification Process.

1.2 SCOPE

This document provides an overview of RTID and the processes required for certifying contributing agencies to submit NPS-NIST compliant electronic transactions to the NPS-NIST Server (RTID system).

1.3 AUDIENCE

This document is intended for the following types of contributing agencies. Note: Hereinafter in this document, all types of contributing agencies may be referred to as “agency” or “agencies”, depending on the context.

- Law Enforcement Agencies
    - e.g. RCMP, Provincial Police, Municipal Police and Military Police that process criminal, civil, and refugee fingerprints, and federal agencies with law enforcement capabilities
- Federal Government Agencies
    - e.g. Public Works and Government Services Canada, Canada Revenue Agency, and other federal agencies that process fingerprints for federal government employment purposes.
- Private Companies
    - e.g. Private sector organizations that have been accredited to take fingerprints for non criminal purposes
- Canadian Criminal Real Time Identification Services (CCRTIS) Operational Support & Client Services personnel

1.4 RELEVANT/REFERENCE DOCUMENTS

- *NPS-NIST ICD for External Contributors*, *Version 1.7.7* (most current revision)
- *SMTP-NIST Message Guidelines: A Companion Document to the NPS NIST External ICD Version 1.7.7*
- *Best Practices for the Capture of Charge Information in Support of NPS-NIST-ICD 1.7.7. (Implementation and Use of the NPS-NIST Charge Table)*[1]
- *Best Practices for the Implementation of Civil Electronic Fingerprint Capture Devices Workflows*
- *RTID Technical Guidelines for Agencies*
- *RTID Security Policy and Guidelines for Non-Law-Enforcement Agencies*
- *RTID Phase 2 Glossary*

1.5 DOCUMENT STRUCTURE

- Section 1 – Overview of the RTID Project and agency certification prerequisites
- Section 2 – Overview of the NPS-NIST Agency Certification Process
- Section 3 – Step-by-step description of the NPS-NIST Agency Certification Process
- Section 4 – CCRTIS Contact Information
- Appendices to document

1.6 RTID AGENCY INFORMATION PACKAGE - DOCUMENTS

RTID Introduction for Agencies

- This document provides an overview of RTID and the NPS-NIST Agency Certification Process. Agency certification prerequisites and testing requirements for RTID are explained in this document.

NPS-NIST ICD for External Contributors, Version 1.7.7 (most current revision)

- This document describes the types and format of information that the RCMP expects to send and receive electronically. Contributing agencies that choose to electronically interface with the RTID system must use the transactions defined in this document.

[1] Law Enforcement Agencies only

SMTP-NIST Message Guidelines: A Companion Document to the NPS NIST External ICD Version 1.7.7

- This document describes the NPS-NIST subsystem interface for Simple Mail Transfer Protocol (SMTP). In addition to providing a logical component view of the interface, this document also describes current system conventions for exchanging transactions.

Best Practices for the Capture of Charge Information in Support of NPS-NIST-ICD 1.7.7. (Implementation and Use of the NPS-NIST Charge Table)

- This document assists vendors and law enforcement agencies in interpreting the NPS-NIST Charge Table, and recommends how the Charge Table structure can be used to help facilitate accurate charge selection and data entry processes required to populate charge information.

Best Practices for the Implementation of Civil Electronic Fingerprint Capture Devices Workflows

- This document provides guidance to vendors and agencies that intend to develop and implement EFCD software for civil purposes that will capture NPS-NIST standard fingerprint submissions and electronically submit NIST packets to the RTID system.

RTID Technical Guidelines for Agencies

- This document provides agencies with an overview of the communications infrastructure and connectivity options between the agency's network and the National Police Services Network (NPSNet) for RTID purposes.

RTID Security Policy and Guidelines for Non-Law-Enforcement Agencies[2]

- This document describes RTID security policy and guidelines for federal government agencies and private fingerprints companies that intend to submit electronic fingerprint transactions to the RTID system.

RTID Glossary

- This document provides definitions of commonly used terms and abbreviations that apply to the RTID Project and to contributing agencies.

[2] Law Enforcement Agencies refer to Chapter 1.4 of the *Canadian Police Information Centre (CPIC) Reference Manual*.

1.7 RTID OVERVIEW

RTID is a two phase Major Crown Project designed to enhance the efficiency of Canada's national fingerprint and criminal record repository. It will replace outdated paper processes and legacy systems with re-engineered workflows and automation. RTID will use modern technology to meet business demands and support interoperability with all clients. RTID efficiencies are directly related to reducing the number of paper-based fingerprint submissions and, in turn, increasing the number of electronic fingerprint submissions.

Fingerprint identification and criminal record services are provided by CCRTIS to the Canadian law enforcement, criminal justice and public security communities, as well as, international partners, such as the Federal Bureau of Investigation (FBI) and Interpol.

1.8 PROJECT SCOPE

There are distinct objectives for both RTID Phase 1 and 2.

RTID Phase 1:

- New Automated Fingerprint Identification System (AFIS)
- New infrastructure for electronic submissions (NPS-NIST Server)
- Automation of civil fingerprint verification processes
- NPS-NIST specification standard for electronic submissions (NPS-NIST ICD)

RTID Phase 2:

- Automation of criminal records processes
- Redesign criminal records workflow component
- Elimination of legacy systems

1.9 SERVICE DELIVERY

When both phases of the RTID Project are fully implemented, response times will be reduced from weeks and months to hours and days. The CCRTIS service delivery response time estimates are indicated below:

1.10 CCRTIS SERVICE DELIVERY RESPONSE TIME ESTIMATES

***RTID Phase 2 SLAs are contingent upon a full RTID implementation. They are not effective at this time.

Service	**Processing Time**		
	2001	**RTID Phase 1**	**RTID Phase 2**
Criminal ten print searches	10 weeks	2 hours	
Latent crime scene searches	5 months	24 hours	
Civil ten print searches (not linked to a criminal record)	6 weeks	72 hours (3 business days)	
Civil ten print searches (linked to a criminal record)	6 weeks		72 hours*** (3 business days)
Criminal record updates	9 months		24 hours***

2 AGENCY CERTIFICATION OVERVIEW

2.1 NPS-NIST AGENCY CERTIFICATION – PREREQUISITE

As a prerequisite to NPS-NIST agency certification, the agency's chosen vendor (e.g. devices and application software) must have undergone and completed NPS-NIST vendor certification.

The NPS-NIST Vendor Certification Process certifies vendor devices for image quality and NPS-NIST-ICD compliancy (e.g. tag/value/character structure). This process tests the vendor's NPS-NIST application software against various electronic submission scenarios that a contributing agency may experience while operational. The vendor's device(s) must be capable of creating and sending NPS-NIST compliant transactions under varying operational circumstances, and be capable of receiving electronic responses. The test cases are based on the tags, values, and character structure as defined in the most recent *NPS-NIST ICD for External Contributors*.

In addition to the aforementioned NPS-NIST compliancy requirements, the vendor's device(s) must:

- be listed on the FBI's IAFIS Certified Products website: https://www.fbibiospecs.org/IAFIS/Default.aspx

Note: Prior to NPS-NIST Agency Certification, the agency is required to provide CCRTIS with copies of certificates and/or other documentation that validates the FBI IAFIS IQS compliancy of the vendor device(s).

2.2 AGENCY CERTIFICATION - OVERVIEW

The NPS-NIST Agency Certification Process ensures that the agency is able to submit NPS-NIST compliant electronic fingerprint transactions over a secure communications infrastructure in a production environment.

An agency's network and security infrastructure is configured prior to migrating an agency to production. Different types of agencies, such as law enforcement agencies and federal government departments, have different network and security requirements for accessing the National Police Services Network (NPSNet). The duration and effort involved with configuring each agency's communications link is dependent upon the type of agency.

2.3 CONSIDERATIONS

The agency is ultimately responsible for submitting NPS-NIST compliant electronic fingerprint transactions to the RTID system. As previously mentioned, agencies must submit transactions in accordance with the most current NPS-NIST ICD specification. In some cases, an agency may intend to submit electronic transactions via an authorized contributor. An example includes arrangements between police services and/or federal government departments for electronically submitting civil fingerprint transactions via an accredited private fingerprinting company to the RTID system. Under these circumstances, an agency would be responsible for all electronic data exchange with the agency that directly connects to the RTID system. It is recommended that an agency advises its applicants of the workflow involved with electronically exchanging data with the RTID system.

Note: The vendor certification process does not represent a test of each and every compliancy requirement of the NPS-NIST-ICD specification and associated business rules. The agency may be required to upgrade their application software and undergo further testing to verify compliancy with the NPS-NIST-ICD specification that was tested, or any new NPS-NIST specification provided by the RCMP. It is understood that should an upgrade be required, the agency will upgrade their application software at their own expense by the date provided by the RCMP, or risk suspension and subsequent termination of their certification. If the agency intends to certify additional devices or new software in accordance with additional transactions and civil application types, further vendor testing will be required.

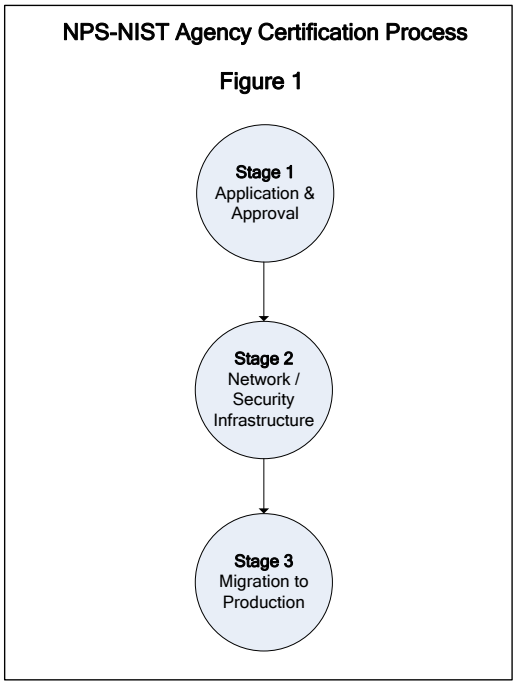
3 NPS-NIST AGENCY CERTIFICATION PROCESS

3.1 AGENCY CERTIFICATION PROCESS - WORKFLOW

The NPS-NIST Agency Certification Process consists of three stages, each of which is comprised of a number of steps. The stages are:

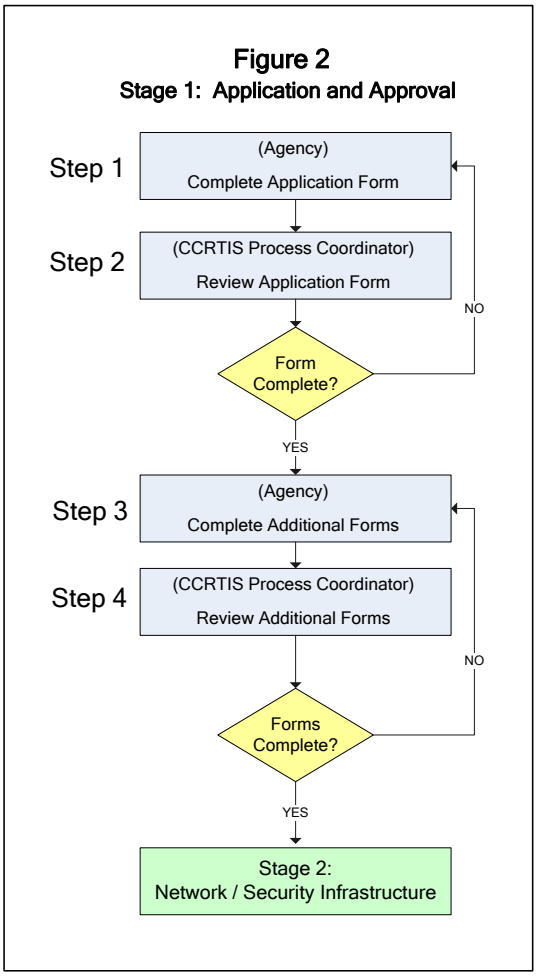
Stage 1	Application and Approval
Stage 2	Network / Security Infrastructure
Stage 3	Migration to Production

Figure 1 provides an overview of the NPS-NIST Agency Certification Process



3.2 AGENCY CERTIFICATION PROCESS – STEPS

Figure 2 provides an overview of **Stage 1 Application & Approval**



Step 1 **Complete Application Form**

Performed by: Agency

Description: The agency completes the NPS-NIST Agency Certification Application Form and submits the form to CCRTIS at: RTID_ITR_Certification@rcmp-grc.gc.ca

The form identifies: contact details; vendor product information; and requested transactions for certification.

Note: Agencies may contact CCRTIS at RTID_ITR_Certification@rcmp-grc.gc.ca to request an e-copy of the NPS-NIST Agency Certification Application Form.

Step 2 **Review Application Form**

Performed by: CCRTIS Process Coordinator

Description: The CCRTIS Process Coordinator reviews the form for accuracy and completeness (e.g. vendor product specifications are complete, FBI IAFIS IQS compliancy is verified, transactions are selected, etc.).

If the form is incomplete, the CCRTIS Process Coordinator sends the form back to the agency and advises of the outstanding information.

When the form is verified as complete by the CCRTIS Process Coordinator, the certification process continues to **Step 3**.

Step 3 **Complete Additional Forms**

Performed by: Agency

Description: Depending on the type of agency, the CCRTIS Process Coordinator sends additional forms that must be completed prior to certification. As an example, all agency types will be required to complete an RTID Network Infrastructure Report, which supports the security and network connectivity requirements for configuring an agency's communications link for operational purposes.

Certain agency types will also be required to complete an RTID Physical Site Inspection and Security Report, which is completed to verify the physical parameters of the agency's Virtual Private Network (VPN) device.

Depending on the type of agency, the aforementioned forms must be completed prior to certification.
Note: Agencies may contact CCRTIS at RTID_ITR_Certification@rcmp-grc.gc.ca to request any additional forms that may be required.

Step 4 **Review Additional Forms**

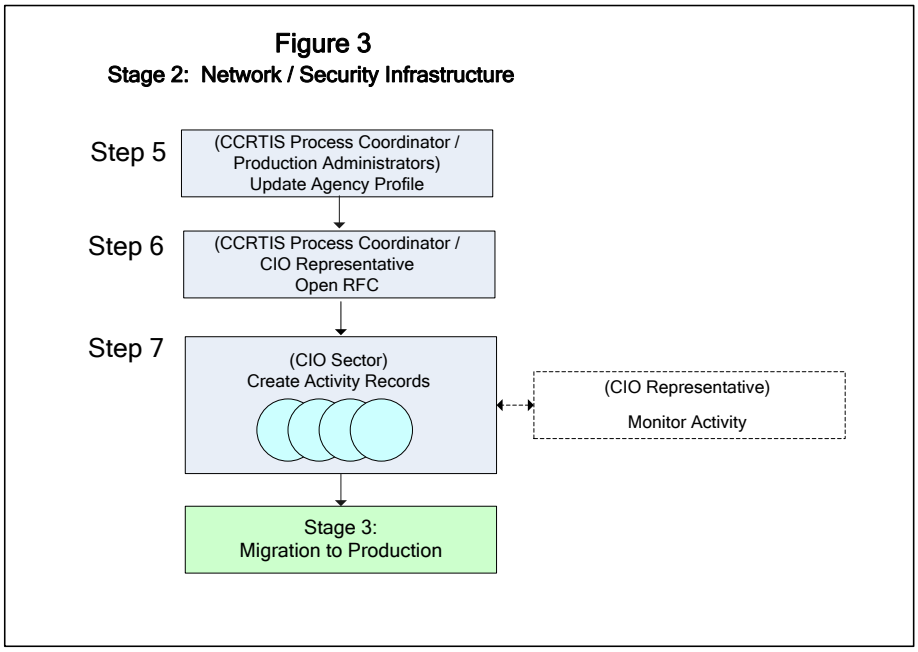
Performed by: CCRTIS Process Coordinator

Description: The CCRTIS Process Coordinator reviews the additional forms for accuracy and completeness. Depending on the type of form, the CCRTIS Process Coordinator may send the forms to other business lines for assessment.

If the forms are incomplete, the CCRTIS Process Coordinator sends the forms back to the agency and advises of the outstanding information.

When the forms are verified as complete by the CCRTIS Process Coordinator, the certification process continues to **Stage 2 – Network / Security Infrastructure**.

Figure 3 provides an overview of **Stage 2 Network / Security Infrastructure**



Step 5 **Update Agency Profile**

Performed by: CCRTIS Process Coordinator
CCRTIS Production Administrators

Description:

The CCRTIS Process Coordinator advises the CCRTIS Production Administrators of the Agency Profile requirements for certification. Updates are made by the Production Administrators. An Agency Profile must be configured in accordance with the agency's operational requirements, and added to the required system applications (e.g. NPS-NIST Server (NNS) Console, Paper Conversion Sub-system). An Agency Profile is used to validate incoming submissions in accordance with an agency's submission authorities. Validation is based on an Agency Identifier (ORI), which is uniquely assigned to each agency
.

Step 6 **Open RFC**

Performed by: CCRTIS Process Coordinator
CIO Representative

Description: The Request for Change (RFC) is required to configure the agency's secure network infrastructure for operational purposes.

Based on the RTID Network Infrastructure Report (Step 3), the CCRTIS Process Coordinator conveys the network requirements for configuring the agency's communications link for the production environment. In turn, the CIO Representative opens an RFC.

The RFC identifies the business sections and technical configuration changes that are required for establishing a branch-to-branch communications link between the agency's network and the NPSNet.

The CIO Representative will advise the CCRTIS Process Coordinator when the RFC is complete, and will directly follow-up with any areas of responsibility if any of the requirements are incomplete.

Note: The effort required to configure the agency's network infrastructure is dependent upon the type of agency. For example, a private company would have their VPN configured with an RCMP Entrust Device Certificate, and would connect to the NPSNet via a Secure Internet connection. A federal government department would enable their VPN with a cross-certified device certificate, and would connect to the NPSNet via a shared VPN tunnel over the Secure Channel InterGov (SCNet) Network[3]. For a law enforcement agency, a reconfiguration of their existing connection to the NPSNet may be required.

Step 7 **Create Activity Records**

Performed by: CIO Sections

Description: The CIO Sections (e.g. Central Region Network Services Section (CRNSS); Network Engineering, Research and Development Section (NERDS); Network VPN; Network Firewall; Enterprise Computing Services (ECS); Operations) open Activity Records and complete the work that is required to establish a branch-to-branch secure network connection between the agency's network and the NPSNet.

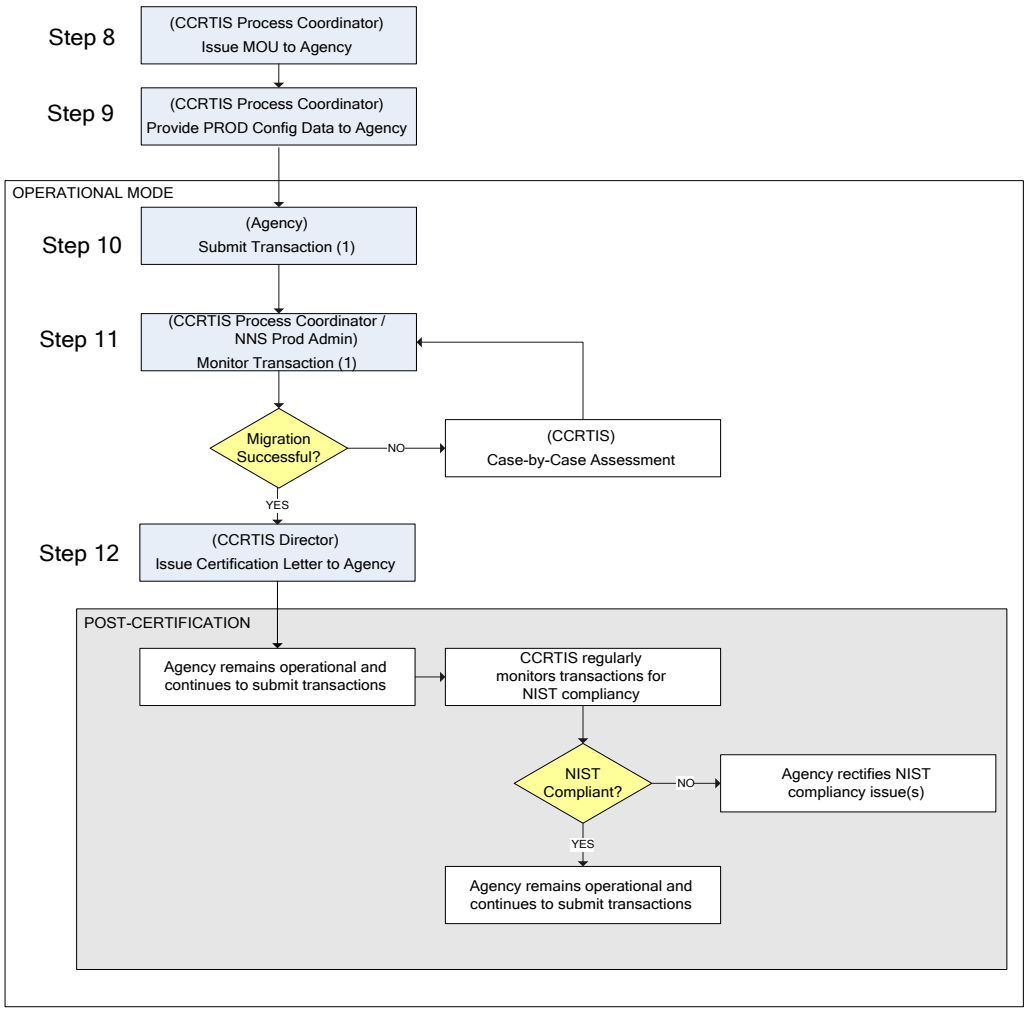
Note: The CIO Sections, work details, and time line for completing the Activity Records are dependent upon the type of agency and the method of connectivity.

[3] Agencies should refer to the *RTID Technical Guidelines for Agencies* document for more information on network connectivity options.

Figure 4 provides an overview of **Stage 3 Migration to Production**

Figure 4

Stage 3 Migration to Production



Step 8 **Issues MOU to Agency (TBD)**

Performed by: CCRTIS Operational Support & Client Services

Description: The CCRTIS Operational Support & Client Services issues a Memorandum of Understanding (MOU) to the agency. The MOU covers the ongoing participating conditions of both the agency and the RCMP. The agency's ongoing participation in RTID must be in accordance with the obligations as set forth in the MOU.

Note: The RCMP and the agency will make their best efforts to make the MOU effective prior to the agency's operational status. At the discretion of the RCMP, the agency may become operational prior to signing the MOU, providing that the agency is actively working towards making the MOU effective.

Note: CCRTIS Operational Support & Client Services is currently developing a reference manual that will outline all access requirements for agencies that connect to the RTID system. The reference manual will eventually support the MOU arrangement between the RCMP and the agency.

Step 9 **Provide Production Configuration Data to Agency**

Performed by: CCRTIS Process Coordinator

Description: The CCRTIS Process Coordinator sends the configuration information that the agency will require to interface with the production environment. The configuration information includes the Originating Agency Identifier (OAI) value that the agency must identify on each submission (Tag 1.008) and the email address that the agency must send to for operational purposes. The Internet Protocol (IP) will be provided by Central Region Network Services Section

Step 10 **Submit Transaction (1)**

Performed by: Agency

Description: The agency submits their initial electronic fingerprint transaction to the production environment. The agency will only initially send one transaction to ensure that the agency has successfully migrated to the production environment.

Formatted: Right

Step 11 **Monitor Transactions (1)**

Performed by: CCRTIS Process Coordinator
NNS Production Administrators

Description: The Certification Process Coordinator and NNS Production Administrators monitor the agency's initial electronic submission to ensure successful migration.

If the agency successfully migrates to the production environment, the agency may continue to submit NPS-NIST compliant transactions. Any identified migration issues will be assessed on a case-by-case basis.

Note: In accordance with the MOU, the agency's electronic submissions will continually be monitored, validated, and audited for NPS-NIST compliancy.

4 CONTACT INFORMATION

Canadian Criminal Real Time Identification Services (CCRTIS)

Email: RTID_ITR_Certification@rcmp-grc.gc.ca

Phone: CCRTIS Process Coordinator - (613) 990-8709

Facsimile: (613) 993-4244

Address: Director General
Canadian Criminal Real Time Identification Services
RCMP, NPS Bldg.
1200 Vanier Parkway
Ottawa, ON
K1A 0R2