Public Reporting of the Core Privacy Impact Assessment:

Real Time Identification System

Atomic Energy of Canada Limited
Access to Information and
Privacy Office

May 2013

CORE PRIVACY IMPACT ASSESSMENT

Table of Content

References

1. Directive on Privacy Impact Assessment, TBS, April 1, 2010 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18308
2. A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century, Office of the Privacy Commissioner of Canada, November 2010.
3. Info Source Publications, Sources of Federal Government and Employee Information 2010, TBS, http://www.infosource.gc.ca/emp/emp00-eng.asp
4. Directive on Privacy Practices, TBS, April 1, 2010, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18309
5. Policy on Privacy Protection, TBS, April 1, 2008, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12510
6. Personnel Security Standard, TBS, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12330&section=text
7. Real Time Identification System Privacy Impact Assessment Summary, Royal Canadian Mounted Police, http://www.rcmp-grc.gc.ca/rtid-itr/pia-efpv-eng.htm
8. *Privacy Ac*t (R.S.C, 1985, c.P-21), Department of Justice, http://laws-lois.justice.gc.ca/eng/acts/P-21/
9. *Canadian Security Intelligence Service Act*, August 31, 2004, http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp
10. *The Nuclear Safety and Control Act*, May 31, 2000, http://laws-lois.justice.gc.ca/eng/acts/N-28.3/index.html
11. AECL's Retention Scheduling policy CW-511300-012-414 Rev. 0
12. Real Time Identification System User Guide, Version 1.0
13. Real Time Identification Technical Guidelines for Agencies, RCMP, 2009-05-15
14. RTID SMTP-NIST Message Guidelines, RCMP, 2008-04-18
15. RTID Best Practices for the Implementation of Civil Electronic Fingerprint Capture Devices Workflows, RCMP, 2009-05-19
16. RTID Security Policy and Guidelines for Non-Law-Enforcement Agencies, RCMP, 2009-08-31
17. RTID Introduction for Agencies, RCMP, 2009-01-19
18. National Institute of Standards and Technology Interface Control Document for External Contributors, RCMP, NPS-NIST-ICD, 2010-07-30, Version 1.7.7 Rev E2

Acronyms and Abbreviations

Acronym / Abbreviations	**Definition**
AECL	Atomic Energy of Canada Limited
ATIP	Access to Information and Privacy
CBSA	Canada Border Services Agency
CRNC	Criminal Records Name Check
CNSC	Canadian Nuclear Safety Commission
CPIC	Canadian Police Information Centre
CRL	Chalk River Laboratories
CSIS	Canadian Security Intelligence Service
FAA	*Financial Administration Act*
HR	Human Resources
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards in Technology
NPS	National Police Services
OPC	Office of the Privacy Commissioner
PA	Program Activity
PAA	Program Activity Architecture
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PSO	Personnel Security Officer
PSS	Personnel Security Services
RCMP	Royal Canadian Mounted Police
RTID	Real Time Identification System
SAS	Security Advisory System
S&T	Science and Technology
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment

Executive Summary

Personal information is necessary to perform reliability checks, security clearances and criminal records verifications. This is required to give AECL employees the access to the work area and the appropriate security clearance for the work to be performed. RTID is a seamless electronic submission of fingerprint data to be used for AECL personnel security screening purposes. The electronic processes planned for RTID are primarily a re-engineering of existing services, meaning that the information received from candidates will change only slightly. Therefore, the PIA focuses on two program elements: the increased collection of personal information, significant changes to the processes and/or systems that affect the physical or logical separation of personal information, and the security mechanisms used to manage and control access to personal information once received by RTID.

The RTID System electronically captures and processes forensic-quality fingerprints and demographic data. The system packages the information into standard, NIST-format files and sends them to the Royal Canadian Mounted Police (RCMP) National Institute of Standards in Technology (NIST)-compatible system.

By automating the fingerprint and criminal record verification processes, RTID will address different challenges AECL's Personnel Security Screening Services currently faces. Transforming the current paper-based infrastructure into a paperless electronic system will allow completing work in only hours that previously took months.

The RTID system is also “Protected B” capable improving the security and protection of the related personal information. All personal information transmitted to and from the RTID system will also be encrypted. AECL has achieved accreditation through RCMP to submit this type of transaction.

The scope of work embodied in this PIA is the implementation of the RTID System. RTID is limited in scope to the receipt and processing of various identification requests, more specifically it will allow for AECL Security to process Civil Security Clearances on existing personnel and potential candidates who may be employed within AECL. The scope of this PIA is limited to an analysis of the collection, use, retention and disclosure of personal information through the RTID System.

Personal information stored in RTID is only accessible by AECL authorized individuals. Sections 10 and 11 of the *Privacy Act* require a government institution to include in Personal Information Banks (PIB) all information under the control of the government institution and to publish an index of all personal information banks within the institution. This information is collected by virtue of PIB AECL PSU 917. The provisions of the *Privacy Act* pertaining to access, collection, accuracy, completeness, and amending incorrect data apply.

Consent of the individual for the collection of fingerprint images is required on civil transactions. The individual's consent is obtained via a separate consent form. Fingerprint images for civil transactions are not retained on the RTID system. They are deleted at the completion of the transaction.

RTID is a highly secure system with extensive security features and procedures. Any functionality released to production undergoes extensive testing to ensure any result generated by RTID adheres to the legislation and policies concerning fingerprint data. Additionally, there are manual procedures and regular audits that ensure the information released for an individual is accurate and sent to only those recipients authorized to receive the information.

In conclusion, the privacy issues identified in this Privacy Impact Assessment (PIA) can be resolved through the development and documentation of appropriate procedures and processes that ensures compliance with the *Privacy Act*. The use of sensitive biometric data through the RTID will only be used for the purpose it is collected. AECL has demonstrated an ongoing commitment to the security and protection of its RTID system and personal information involved.

1 SECTION I - OVERVIEW & PIA INITIATION

Government Institution

Atomic Energy of Canada Limited (AECL)

Officials Responsible for the Privacy Impact Assessment (PIA)	Head of the institution / Delegate for section 10 of the *Privacy Act*
Lee-Anne Johns, Personnel Security Services Program Coordinator Jean Boulais, Director of Access to Information and Privacy	Dr. Robert Walker, President and Chief Executive Officer

Name of program or activity of the government institution

Personnel Security Services – Real Time Identification System (RTID)

1.1 Description of the Program or Activity:

Personal information is necessary to perform reliability checks, security clearances and criminal records verifications. This is necessary to give AECL employees the access to the work area and the appropriate security clearance for the work to be performed. RTID is a seamless electronic submission of fingerprint data to be used for AECL personnel security screening purposes. The RTID System electronically captures and processes forensic-quality fingerprints and demographic data. The system packages the information into standard, NIST-format files and sends them to the Royal Canadian Mounted Police (RCMP) National Institute of Standards in Technology (NIST)-compatible system. By automating the fingerprint and criminal record verification processes, RTID will address different challenges AECL's Personnel Security Screening Services currently faces. Transforming the current paper-based infrastructure into a paperless electronic system will allow completing work in only hours and days that previously took weeks and months. The RTID system is "Protected B" capable improving the security and protection of personal information. All personal information transmitted to and from the RTID system will be encrypted.

Aligned with AECL's Program Activity Architecture (PAA) and also described in AECL's 2010-2011 Info Source Chapter, AECL's Personnel Security Screening Services will operate the RTID under the Program Activity (PA) 2001121 Internal Services, Personnel Security Screening as following:

PA 2001121 – INTERNAL SERVICES: Internal Services are groups of related activities and resources that are administered to support the needs of programs and other corporate obligations of an organization. These groups are: Management and Oversight Services; Communications Services; Legal Services; Human Resources Management Services; Financial Management Services; Information Management Services; Information Technology Services; Real Property Services; Material Services; Acquisition Services; and Travel and Other Administrative Services. Internal Services include only those activities and resources that apply across an organization and not to those provided specifically to a program.

HUMAN RESOURCES MANAGEMENT

Human Resources Management Services involve activities undertaken for determining strategic direction, allocating resources among services and processes, as well as activities relating to analyzing exposure to risk and determining appropriate countermeasures. They ensure that the service operations and programs of the federal government comply with applicable laws, regulations, policies, and/or plans.

- Recruitment and Staffing
  - ➢ Personnel Security Screening

TRAVEL AND OTHER ADMINISTRATIVE SERVICES

Travel and Other Administrative Services include Government of Canada (GC) travel services, as well as those other internal services that do not smoothly fit with any of the internal services categories.

- Security
  - ➢ Personnel Security Screening

1.2 Description of the class of records associated with the program or activity:

AECL's Access to Information and Privacy Office is responsible for providing a full accounting of information holdings to the Treasury Board Secretariat for inclusion in the Info Source publication. The Info Source publication contains a description of the classes of institutional records by AECL. Descriptions of the records created, collected and maintained by Personnel Security Screening can be found under the following classes of records.

Recruitment and Staffing:
Description: Includes records related to the recruitment and staffing of people to fill full-time or part-time positions within the institution. Records may include information related to screening, examining, testing, interviewing, assessing, selecting, hiring, and promoting candidates for employment. May also include information related to terms and conditions of employment (including conflict of interest), deployments, assignments, and secondments, student, professional, and occupational recruitment, post-employment appeals, and area of selection, as well as information received from or shared with central agencies responsible for recruitment and staffing, other employment agencies, or both. ***Note:*** Relevant information may be transferred to an employee's personnel file if the individual accepts an offer of employment from the institution.
Document Types**:** Unsolicited résumés and curricula vitae, model interview questions and answers, competition posters and announcements, application forms, competition assessment tools and rating guides, reference check procedures, checklists, and letters, inventories of qualified candidates (including pre-qualified pools), candidate inquiries and responses, copies of letters of offer, ratings board assessments, information within automated or Web-based application tools, and second language evaluation results, etc.
Record Number: PRN 920

Security
Description*:* Includes records related to the application of safeguards to protect employees, preserve the confidentiality, integrity, availability and value of assets, and assure the continued delivery of services from accidental or intentional damage or from unauthorized access. Records may include information related to facilities' design, physical safeguards, monitoring devices, access to restricted zones, storage, transportation and transmittal of information and goods, work-related violence, protected and classified information, entry and exit points, emergency services, signage, identification cards and/or access badges, personnel security screening, continuous security risk management, building and fire codes, and destruction of information and goods. May also include records related to liaison with other federal institutions that have security-related responsibilities (for example, the Canadian Security Intelligence Service, Public Safety Canada, RCMP, Communications Security Establishment, etc.)

Document Types*:* Security access procedures and tools (access pass/identity cards), security incidents investigation reports, security training, copies of Threat and Risk Assessments (TRA), awareness and briefings documentation, security clearance records, incident response procedures, security program audit reports, baseline security requirements, evacuation plans, operational standards and technical documentation, business impact analyses, and copies of relevant labour, fire, building and electrical regulations and codes.
Record Number: PRN 931

1.3 Existing standard personal information bank – Personnel Security Screening

Sections 10 and 11 of the *Privacy Act* require a government institution to include in Personal Information Banks (PIB) all information under the control of the government institution and to publish an index of all personal information banks within the institution. RTID information is collected by virtue of Personnel Security Screening PIB AECL PSU 917, registration number 7193.

Personnel Security Screening
TBS Registration Number – 7193
Description: This bank describes information that is related to security screening assessments of individuals working or applying for work with a government institution. Personal information may include name(s), contact information, biographical information, biometric information (e.g., fingerprints, digital photographs, etc.), character assessments (e.g., loyalty, trustworthiness, etc.) citizenship status, credit information, criminal checks/history, date of birth, educational information, employee identification number, employee personnel information, financial information, other identification numbers, opinions and views of, or about, individuals, physical attributes, place of birth, signature, and military service information. The bank may also describe personal information about any immediate relatives, including name, contact information, date of birth and death, and relationship to applicant.
Note: The Department of National Defence (DND), the Royal Canadian Mounted Police (RCMP), and the Canadian Security Intelligence Service (CSIS) have established the following institution-specific personal information banks to account for information used in the security/reliability screening of their own employees: DND, Personnel Security Investigation File - DND PPE 834; RCMP, Security/Reliability Screening Records - CMP PPE 065; CSIS, Employee Security - SIS PPE 815. In addition, Public Works and Government Services Canada (PWGSC) has established the following institution-specific personal information bank to account for information used in the security/reliability screening of private sector industry personnel: Industry Personnel Clearance and Reliability - PWGSC PPU 015.
Class of Individuals: General public, including volunteers, all current and former employees, contractors, immediate relatives, current and former spouse/common law partner, agency, casual employees, and students, individuals who give character references (including neighbours), current/former employers.
Purpose: Personal information is used to support decisions for granting or reviewing for cause the reliability status, security clearance or site access of individuals working or applying to work through appointment, assignment or contract. A review for cause may result in the revoking of the individual's reliability status, security clearance or site access. For many institutions, personal information is collected pursuant to subsection 7(1) of the Financial Administration Act (FAA) and as required under the Policy on Government Security. For those institutions not subject to the FAA or the Policy on Government Security, consult the institution's Access to Information Coordinator to determine collection authority.
Consistent Uses: Where applicable, information, including fingerprints, may be shared with the RCMP and CSIS to conduct the requisite checks and/or investigation in accordance with the Policy on Government Security; refer to the following institution-specific personal information banks: for the RMCP, Forensic Science and Identification Services and Canadian Criminal Real Time Identification Services - CMP PPU 030; for CSIS, Security Assessments/Advice - SIS PPU 005. The security screening status may be shared with Human Resources officials to update the individual's personnel file, refer to Standard Personal Information Bank Employee Personnel Record - PSE 901. Information may be shared with entities outside the federal government, including credit bureaus. Some information may be used or disclosed for program evaluation.
Retention and Disposal Standards: For information about the length of time that specific types of common administrative records are maintained by a government institution, including the final disposition of those records, please contact the institution's Access to Information and Privacy Coordinator.
RDA Number: 98/001
Related Class of Record Number: PRN 920 and PRN 931
Bank Number: AECL PSU 917

1.4 Legal Authority for the Program Activity:

Atomic Energy of Canada Limited was incorporated in 1952 under the provisions of the *Canada Corporations Act* (and continued in 1977 under the provisions of the *Canada Business Corporations Act*), pursuant to the authority and powers of the Minister of Natural Resources under the *Nuclear Energy Act*. On September 1st, 2007 the *Federal Accountability Act* amended the *Access to Information Act* and *Privacy Act* to include AECL.

The Corporation is a Schedule III Part I Crown corporation under the *Financial Administration Act* and an agent of Her Majesty the Queen in Right of Canada. The collection of personal information for the purpose of security clearances is given authority under subsections 7(1) and 11.1(1) of the *Financial Administration Act.*

AECL Personnel Security Services are also responsible in conducting personnel screening in compliance with Treasury Board of Canada Secretariat Policy on Government Security ref. 2-4 - Personnel Security Standard and section 18.1 of the *Nuclear Security Regulations*.

1.5 Summary of the project / initiative / change:

AECL's Business Objectives

AECL is aligned to a single Strategic Outcome: Canadians and the world receive energy, health, environmental and economic benefits from nuclear science and technology, with confidence that nuclear safety and security are assured.

Following the federal Science and Technology (S&T) strategy, AECL contributes to Canada's knowledge advantage by pursuing this Strategic Outcome. The knowledge advantage emphasizes research on fields within S&T that are going to be strategically important in the future. It also emphasizes research in fields where Canada has an established strength. On both bases nuclear S&T is well-positioned to improve the quality of life for Canadians.

PIA Objectives

This report is a Privacy Impact Assessment for the RTID system purchased by AECL to be installed in Chalk River and Whiteshell Laboratories. The PIA will ensure that privacy is considered throughout the acquisition and implementation of the RTID. This is documented assurance that privacy issues have been identified and adequately addressed.

The Objectives of this PIA are:

- To review the business processes to identify the data flow of personal information;
- Analyze the collection, use, disclosure and retention of personal information;
- To determine if there are privacy issues or risks associated with the implementation of the RTID System;
- To recommend measures to avoid, control and mitigate any privacy issues or risks.

The information presented in this report follows the format of the Treasury Board Secretariat's Directive on Privacy Impact Assessment and OPC's guidance document "*Expectations: A Guide for*

Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada".

The TBS Directive on Privacy Impact Assessment came into effect on April 1, 2010 and applies to government institutions as defined in section 3 of the *Privacy Act,* including parent Crown corporations.

Project Scope

The scope of work embodied in the PIA is the implementation of the RTID System. RTID is limited in scope to the receipt and processing of various identification and related requests, more specifically it will allow for AECL Security to process Civil Security Clearances on existing personnel and potential candidates who may be employed within AECL. The scope of this PIA is limited to an analysis of the collection, use, protection, retention and disclosure of personal information in the RTID System.

It would be beneficial for AECL to take potential employees fingerprints while they are onsite for their interview and utilize a written consent form (Appendix A) to enable us to capture their fingerprints. The personnel security data will be electronically transmitted to the RCMP for verification. RTID will help expedite the clearance process using National Institute of Standards in Technology (NIST) standards.

Applicants being considered for employment within AECL must be security cleared prior to commencing employment. AECL currently utilizes the 400X system Royal Canadian Mounted Police (RCMP) Canadian Police Information Centre (CPIC) to gain the criminal record information.

AECL pursued the purchase of a Livescan fingerprinting device (RTID) to enable Personnel Security Screening Services to electronically submit fingerprints to receive replies back in 48-72 hours as opposed to sending hard copy prints which take 8-12 weeks for replies. In the past (prior to 911) our regular process was to send in fingerprints for all employees and contractors. AECL will be using the RTID technology in Whiteshell & Chalk River Laboratories. The systems have achieved accreditation through RCMP and meet NPS-NSIST-ICD requirements (see appendix E). Certification ensures that transactions are correctly formatted and contain all the required content.

Project Initiative

In 1968, National Police Services (NPS) installed the world's first Automated Fingerprint Identification System (AFIS). Since then, NPS has used various generations of AFIS and other technologies to perform electronic searches of incoming ten print[1] and latent[2] fingerprints against criminal fingerprint databases. Other systems such as the Criminal Name Index (CNI), the Criminal History System (CHS), Criminal Record Editing, Maintenance and Monitoring System (CREMMS) and CREMMDES (remote version of CREMMS) have helped expedite electronic processing[3]. Though efficient, these systems are not interfaced with one another and were developed in isolation of other law enforcement systems. The processing of submissions also requires extensive duplication of data entry. These processes are complex, labour intensive and cannot produce results in the time required by clients. The Auditor General of Canada's 2000 report highlighted these shortcomings (Section 3.3 of this document). RCMP senior management has been committed to resolving these issues since 2000, providing significant resources to defining the business requirements for an electronic system, and identifying four options in a business case.

In reaching its objectives, RTID will significantly reduce the time required to verify and update

[1] A ten print is a full set of ten rolled fingerprints that is typically received with a criminal charge on a C-216.
[2] A latent fingerprint is a fingerprint that has been lifted from a crime scene.
[3] See Appendix A for more details of the current systems.

information. The following illustrates the type of service improvement that RTID will provide AECL. Today, AECL completes a civil clearance by:

a) Personnel Security Screening Office receives personnel screening package from HR;
b) Complete Personnel Screening, Consent and Authorization form TBS/SCT 330-23E and ensure that the document and reference checks have been signed off by HR and the applicant;
c) If form is not signed Personnel Security Officer (PSO) will obtain verbal or written consent from the applicant;
d) Applicants information is captured in the Security Advisory Systems (SAS) by PSO:
e) Conduct a certified criminal records name check (CRNC) with the RCMP utilizing the 400X;
f) If the reply from the RCMP is incomplete, a CRNC request is forwarded to DRPS;
g) If the results indicate a criminal conviction other than what is self reported, fingerprints are required;
h) If fingerprints are required the PSO will contact the applicant and advise the requirement for him/her to have fingerprint identification conducted by the local police station;
i) The local police will complete RCMP fingerprint form (C-216C (88-12) 7540-21-862-7891) and sends it to RCMP for criminal checks (See Diagram 1 for RCMP current manual/automated paper-based workflow vs RTID automated workflow in Civil Security Clearance Request);
j) Applicant is responsible for submitting criminal check results to Personal Security Services
k) If RCMP results is adverse information the file is forwarded to the Personnel Security Program Coordinator for a subject interview and risk management assessment;
l) If RCMP results indicate no adverse information, reliability check is granted;
m) A Security Screening Certificate (TBS/SCT 330-47) is completed and signed by Personnel Security Officer or the Personnel Security Program Coordinator;
n) Email notification is sent to HR and Information Technology (IT) advising individual is security cleared;
o) To be eligible to be granted a Level 1, Level 2, Level 3 or Site Access Clearance, all requirements of the Reliability Check must be met.

In addition to the Reliability Check steps A to K above, the following steps occur for a Level 2, Level 3 and/or Site Access Clearance with the exception of steps F to I which are not applicable for Level 3 clearances as PSS currently utilizes the RTID for Level 3 clearance only as it is a Treasury Board requirement to submit fingerprints for Level 3:

a) PSO reviews Site Access Questionnaire or Security Clearance Form (TBS/SCT 330-60E) for completion, missing information and signatures.
b) In addition to the CRNC, PSO will conduct a credit report for Level 2 and Level 3 clearances;
c) Applicants information is captured in the Security Advisory System (SAS) by the PSO;
d) PSO enters applicants information in the Security Screening Information System (SSIS) specific to the level of clearance;
e) PSO exports applicants information from SSIS to the Canadian Security Intelligence Service (CSIS)
f) Results from CSIS can be up to 10 business days or longer depending on the information submitted.
g) PSO will import results from CSIS upon receipt of encrypted file;
h) If CSIS results are “Incomplete”, file is forwarded to the Personnel Security Services Program Coordinator for a subject interview and risk management assessment
i) If CSIS results received are “No Reportable Traces”, clearance is granted;
j) A Security Screening Certificate TBS/SCT 330-47 is completed and signed by PSO or the Personnel Security Program Coordinator;
k) Email notification is sent to HR and IT advising individual is security cleared;
l) Individual is scheduled for Security Clearance briefing and issued AECL access card after

applicable AECL training is completed.

Steps to completing a clearance using RTID:

a) Applicant attends interview process with HR and/or interview panel;
b) Applicant is brought to Personnel Security Screening Services (PSS) for briefing on the Fingerprint Identification Consent Form. Conditions are explained as outlined in Appendix A. Form is signed by applicant and PSO;
c) Personnel Security Officer utilizes the RTID Scanner to fingerprint applicant. The record is held in the RTID log;
d) Once AECL/HR receives the signed letter of offer from the applicant, PSO accesses the RTID log and submits applicants fingerprints electronically to RCMP via Commissionaires server;
e) Unsuccessful applicant's records are deleted from the RTID log;
f) Successful applicant's personnel screening package is received from HR;
g) Ensure Personnel Screening, Consent and Authorization TBS/SCT 330-23E form is complete and that the document and reference checks have been signed off by HR and the applicant;
h) Applicants information is captured in the Security Advisory System (SAS) by PSO;
i) Personnel Security Officer retrieves results from the RTID;
    I. No adverse information within 24 to 48 hours
    II. Adverse information within 48 to 72 hrs unless applicant is before the courts then time delays can occur.
j) Fingerprints and criminal records results are printed and placed on the Personnel Security file of the individual then deleted from RTID;
k) If results have adverse information the file is forwarded to the Personnel Security Program Coordinator for a subject interview and risk management assessment;
l) If results indicate no adverse information, reliability check is granted;
m) A Security Screening Certificate TBS/SCT 330-47 is completed and signed by Personnel Security Officer or the Personnel Security Program Coordinator;
n) Email notification is sent to HR and IT advising individual is security cleared;
o) To be eligible to be granted a Level 1, Level 2, Level 3 or Site Access Clearance, all requirements of the Reliability Check must be met. In addition to the steps for completing a clearance using RTID Steps A to J listed above for Level 2, Level 3 and Site Access would also be completed.

RTID will integrate the electronic processing of fingerprints and criminal records. Today, these two activities are treated as separate functions. RTID will integrate the current set of "stove pipe" systems (separate systems that do not share data through a common database) used to support criminal record and fingerprint information.

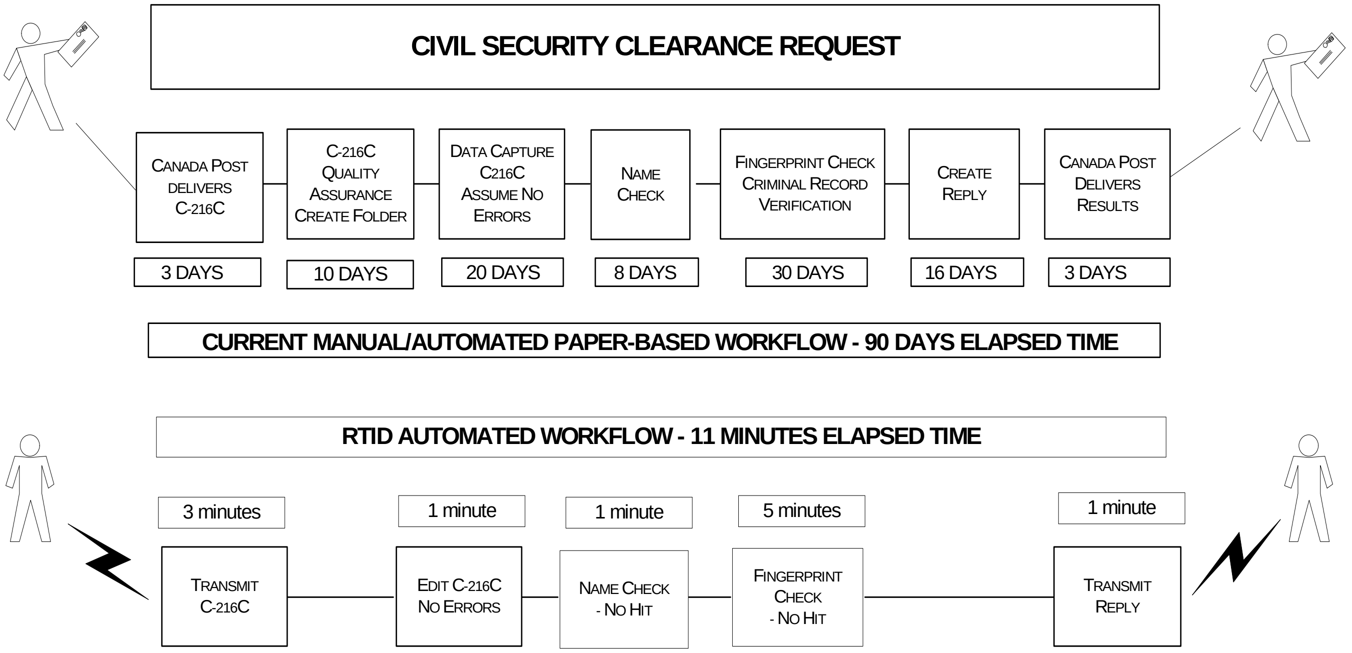
CIVIL SECURITY CLEARANCE REQUEST
CANADA POST DELIVERS C-216C
3 DAYS
C-216C QUALITY ASSURANCE CREATE FOLDER
10 DAYS
DATA CAPTURE C216C ASSUME NO ERRORS
20 DAYS
NAME CHECK
8 DAYS
FINGERPRINT CHECK CRIMINAL RECORD VERIFICATION
30 DAYS
CREATE REPLY
16 DAYS
CANADA POST DELIVERS RESULTS
3 DAYS
CURRENT MANUAL/AUTOMATED PAPER-BASED WORKFLOW - 90 DAYS ELAPSED TIME
RTID AUTOMATED WORKFLOW - 11 MINUTES ELAPSED TIME
3 minutes
TRANSMIT C-216C
1 minute
EDIT C-216C NO ERRORS
1 minute
NAME CHECK - NO HIT
5 minutes
FINGERPRINT CHECK - NO HIT
1 minute
TRANSMIT REPLY

Diagram 1 - RCMP Civil Security Clearance Request Workflow

Benefits of the RTID system

- Resolve the risks to the public and Canadian law-enforcement and justice systems caused by outdated criminal records on CPIC;
- Resolve the RCMP's inability to process civil security clearances in an acceptable length of time; The Smart Border initiative led by the Canada Border Services Agency (CBSA) and other civil security initiatives have created demands and response time expectations that the RCMP is unable to achieve. It presently takes an average of 3 months to process a civil clearance request. The criminal record name check information is always received in a timely manner. If there is adverse information, and hard copy of fingerprints are required, the delays can be up to 8 to 12 weeks.
- Meet security requirements: the current process (paper-based) is not capable of operating in a Protected "B" environment. RTID will be protected "B" environment
- Provide a disaster recovery/business resumption capability to the fingerprint identification: The current system's reliance on paper would make disaster recovery extremely difficult, if not impossible.
- Send transactions encrypted. All personal information transmitted to RCMP from the RTID will be encrypted.

2 SECTION II - RISK AREA IDENTIFICATION & CATEGORIZATION

A: Type of Program or Activity	Level of Risk to Privacy
Program or activity that does NOT involve a decision about an identifiable individual Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual. The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information.	□ 1
Administration of Programs / Activity and Services Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc…).	□ 2
Compliance / Regulatory investigations and enforcement Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e., a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).	☒ 3
Criminal investigation and enforcement / National Security Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).	□ 4

B: Type of Personal Information Involved and Context	Level of risk to privacy
Only personal information provided by the individual – at the time of collection –- relating to an authorized program & collected directly from the individual or with the consent of the individual for this disclosure / with no contextual sensitivities. The context in which the personal information is collected is not particularly sensitive. For example: general licensing, or renewal of travel documents or identity documents.	□ 1
Personal information provided by the individual with consent to also use personal information held by another source / with no contextual sensitivities after the time of collection.	□ 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual. For example: the personal information by association indirectly reveals information on the health, financial situation, religious or lifestyle choices of the individual.	□ 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive. For example: the personal information by association indirectly reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and other individuals, such as relatives.	☒ 4

C: **Program or Activity Partners and Private Sector Involvement**	**Level of risk to privacy**
Within the institution (amongst one or more programs within the same institution)	□ 1
With other federal institutions	☒ 2
With other or a combination of federal/ provincial and/or municipal government(s)	□ 3
Private sector organizations or international organizations or foreign governments	□ 4

D: **Duration of the Program or Activity**	**Level of risk to privacy**
One time program or activity Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.	□ 1
Short–term program A program or an activity that supports a short-term goal with an established "sunset" date.	□ 2
Long-term program Existing program that has been modified or is established with no clear "sunset".	☒ 3

E: **Program Population**	**Level of risk to privacy**
The program affects certain employees for internal administrative purposes.	□ 1
The program affects all employees for internal administrative purposes.	□ 2
The program affects certain individuals for external administrative purposes.	☒ 3
The program affects all individuals for external administrative purposes.	□ 4

F: **Technology and Privacy**	**Risk to privacy**
1. Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	☒ YES □ NO
2**.** Does the new or modified program or activity require any modifications to IT legacy systems and / or services?	□ YES ☒ NO
3. The new or modified program or activity involve the implementation of one or more of the following technologies:	

3.1 Enhanced identification methods This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc…) as well as easy pass technology, new identification cards including magnetic stripe cards, “smart cards” (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic). Identify the applicable category(ies): Fingerprint and Facial Photo	☒YES □ NO
3.2 Use of Surveillance: This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc… Identify the applicable category(ies):	□YES ☒ NO
3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques: For the purposes of the Directive on PIA, government institution are to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behavior. Identify the applicable category(ies):	□YES ☒ NO
A **YES** response to any of the above indicates the potential for privacy concerns and risks that will need to be considered and if necessary mitigated.	

G: <u>Personal Information Transmission</u>	**Level of risk to privacy**
The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	☒ 1
The personal information is used in system that has connections to at least one other system.	□ 2
The personal information is transferred to a portable device or is printed. USB key, diskette, laptop computer, any transfer of the personal information to a different medium.	□ 3
The personal information is transmitted using wireless technologies.	□ 4

H: <u>Risk Impact to the Institution</u>	**Level of risk to privacy**
Managerial harm.	□ 1

Processes must be reviewed, tools must be changed, change in provider / partner.	
Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	☒ 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	□ 3
Reputation harm, embarrassment, lost of credibility. Decrease confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.	□ 4

I: Risk Impact to the Individual or Employee	**Level of risk to privacy**
Inconvenience.	□ 1
Reputation harm, embarrassment.	☒ 2
Financial harm.	□ 3
Physical harm.	□ 4