

CORE PRIVACY IMPACT ASSESSMENT FOR:

Communications Security Establishment Security Information Managed Online System (SIMON) 2.0

CSE-CST

CHANGE CONTROL TABLE

Version	Date	Change Made By	Change Requested By	Change
V 1	June 13, 2012			Original.
V 2	June 14, 2012			Ongoing development of document.
V 3	Sept 10 2012			Sanitised version of CERRID #986537.
V 3.1	October 2012		Unclassified version of PIA	Sanitised version of CERRID #986537
V 4.	October 2012			Review of PIA: <ul style="list-style-type: none"> Confidential version of CERRID #1052563 (V6) and recommendations from TS version of CERRID #986537
V 6.	Dec		Edits	
V 7	October 2013			Development of Executive Summary and draft Info Source text
V 8	December 2013		Privacy Compliance Review	Edits
V 9	May 2014		SA&A process	Clean up and update document. This version is derived from CERRID #1052563, which was derived from CERRID #986537 (from Core PIA TBS template CERRID #978489).
V 10	September 2014		Added review notes for meeting with to determine PIA/TBS/OPC requirements	
V 11	January 2015			Clean up and update document. Final CSD draft for review by the Privacy Office at CSE.
V 12	October 2015			Final draft with responses to comments.
V 13	Jan 2016			Added a table in the Recommendations section to identify how privacy mitigations were implemented. Also made other minor changes.
V 14	Jan 2016			Minor wording changes.
V 15	June 2016			Privacy compliance review and comments.
V 16	June 2016			Edits to address ATIP comments.

V 17	July 2016			Edits to address ATIP comments and additional revisions for clarity.
V 18	October, December 2016			Final edits to address ATIP recommendations and minor editorial changes.
V 19	1 March 2017		Nabih Eldebs	To upgrade classification to SECRET
V20	21 March 2017		Dominic Rochon	Minor edits.

Table of Contents

Change Control Table.....	i
PREAMBLE.....	ii
Executive Summary.....	ii
SECTION I – Overview and PIA Initiation	I
SECTION II – Risk Area Identification and Categorization.....	4
SECTION III – Analysis of Personal Information Elements.....	10
SECTION IV – Flow of Personal Information	14
SECTION V – Privacy Compliance Analysis.....	23
SECTION VI - Summary of Analysis and Recommendations.....	33
SECTION VII – Supplementary Documents List.....	38
SECTION VIII – Approval.....	39
SECTION IX – Appendices.....	40
Appendix A - Glossary of Terms and Acronyms.....	40

PREAMBLE

The Treasury Board Secretariat (TBS) Core Privacy Impact Assessment (PIA) template was used to produce this PIA for the Communications Security Establishment's (CSE) Corporate Security Directorate. The PIA assesses personal information management in the Security Information Managed Online system (SIMON 2.0).

The PIA was initiated in 2012 as part of the Security Accreditation and Authorization (SA&A) process, and has been updated in alignment with the development of the SIMON 2.0 system, its related data stores, and associated applications.

This is the SECRET version. For details please contact the Manager, Access to Information and Privacy Office, CSE.

EXECUTIVE SUMMARY

The Personnel and Physical Security programs within the Corporate Security Directorate (CSD) at CSE provide assurance on the trustworthiness, reliability, suitability and loyalty of individuals who are starting or continuing work at CSE through means of security screenings and associated activities.

The Security Information Managed Online System (SIMON 2.0) is CSE's personnel security information electronic database. The system serves a dual purpose:

- SIMON 2.0 functions as the main information management system that supports the CSD program in conducting personnel security screening for Top Secret clearance and control of SIGINT Access; and
- In its role as the National SIGINT authority for the Government of Canada, CSE uses SIMON 2.0 as the system of record to store the data for all indoctrinations pertaining to the National SIGINT Registry. This enables CSE in its mandate to prevent unauthorized access to sensitive, compartmented information, systems, or locations.

Legal and Policy Framework

The *Library and Archives of Canada Act* governs the management of information within the Government of Canada, including the management of personnel security screening information contained in the SIMON 2.0 repository.

In accordance with Section 7.1 of the *Financial Administration Act (FAA)* and the *Policy on Government Security (PGS)*, CSE collects information for the purposes of personnel security screening under the Personnel and Physical Security programs. The *National Defence Act (NDA)*, *Security of Information Act (SOIA)* and the *CSSS-100: SIGINT Protection and Control* policy authorize the collection of indoctrination information for the purposes of managing the National SIGINT Registry.

SIMON 2.0 Personnel Security Screening Function:

SIMON 2.0 disseminates, retains, and disposes of personal information for the purposes of the personnel security screening process in alignment with the TBS *Policy on Government Security (PGS)* and the *Standard on Security Screening*. Additionally, some security screenings may contain a polygraph assessment and a psychological assessment. The information is stored by the Physical and Personnel Security programs in the Standard TBS Personal Information Bank, PSU 917 (Personnel Security Screening).

SIMON 2.0 National SIGINT Registry Function:

The system also disseminates, retains, and disposes personal data pertaining to CSE applicants, contractors, employees, students, secondees, integrees and other Government of Canada (GoC) employees and contractors who hold SIGINT indoctrination. Information stored includes indoctrination eligibility, status, and de-indoctrination.

The PIA analyses third-party access to personal information stored in SIMON 2.0. The information sharing with the

and other government departments is limited and controlled. The information is basic, protected, and retained in the secure area using comprehensive agreements for use and access.

Summary of Recommendations:

The privacy compliance analysis concludes that the level of privacy risk posed by the system is rated at The risks are effectively mitigated using the security standards for information repositories, which cover the physical, technical and administrative information processing and handling measures.

The recommendations from the PIA are being addressed with the following administrative and technical measures to safeguard the personal information in the system, including:

- Instructions and procedures governing the use of SIMON 2.0;
- Retention and disposition schedules for the personal information created, accessed, disclosed, and stored in the system;
- Ongoing training for CSD employees on privacy and security;
- Implementation of the *SIMON 2.0 User Access Terms and Conditions Agreement* (which includes a briefing on privacy obligations for users);
- and
- Control measures to limit access to the system based on job requirements and need-to-know.

Based on the results of the PIA, CSE demonstrates its commitment to ensuring strong privacy protections are part of the design and implementation of the SIMON 2.0 system.

SECTION I – OVERVIEW AND PIA INITIATION**Government Institution: Communications Security Establishment (CSE)**

Program Authority Responsible for the Privacy Impact Assessment	Head of the government institution / Delegate for section 10 of the <i>Privacy Act</i>
The Official accountable for the Personnel and Physical Security Programs and the SIMON 2.0 System is the Director General, Corporate Services Operations (DGCS OPS).	The Delegated Authorities for the administration of the <i>Privacy Act</i> at CSE are the Director, Disclosure Policy and Review (Dir, DPR) and Deputy Chief, Policy and Communications (DCPC).

Name of Program or Activity of the Government Institution: Personnel and Physical Security
Description of System¹:

The Security Information Managed Online System (SIMON 2.0) is the updated application built to support the CSE Personnel and Physical Security Programs and the National SIGINT Registry.

SIMON 2.0 is CSE's personnel security information electronic database and also serves as the National SIGINT Registry. The system contains personal data pertaining to CSE applicants, contractors, employees, students, secondees, integrees and other Government of Canada (GoC) employees and contractors who may hold SIGINT indoctrination. This information held is used to facilitate the screening, clearance processing and recording of clearance/indoctrinations/de-indoctrination status and security violations pertaining to GoC personnel. Data within this system may be sourced from and shared with other departments and organizations in compliance with authorized derivative use purposes.

- Proposal for a New Personal Information Bank
- Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description

Summary of the project / initiative / change

This PIA was motivated by the replacement of the legacy Security Information Management (SIMON) system with the new SIMON 2.0 upgrade. The implementation of the upgrade to SIMON 2.0 has improved the Personnel Security processes for screening and indoctrinations. It has resulted in streamlining the process for capturing the data and improved data accuracy, while providing timely

¹ Where possible, all references to the "Program or Activity" have been replaced by "System", as the scope of this PIA is limited to assessing the management of personal information in the SIMON 2.0 application. The Personnel Security Screening program PIA will be a separate exercise, considering the anticipated changes resulting from the upcoming in 2016/2017.

and reliable data for measuring performance. It possesses enhanced abilities to support management decisions, improve accessibility to Official Records, and provides to internal and external stakeholders in a secure, protected environment.

Note that the upgrade to SIMON 2.0 **does not reflect** an additional collection or a new use of personal information contained in the system. It represents an improvement to **information management**, allowing for automated digitization and retention and disposition of the information in the system.

The Security Information Managed Online System (SIMON 2.0) has:

- Improved the service level of efficiency by:
 - 1) Providing workflow guidance and tracking;
 - 2) Providing enhanced Auditing capability; and
 - 3) Implementing an intuitive user GUI interface.
- Reduced the time and effort to respond to service requests for Security Clearance and Indoctrinations by automating the business processes;
- Increased efficiency in managing and processing Corporate Security information by having a single application to enter information;
- Maintained data integrity and accuracy of captured data by:
 - 1) Structuring the data
 - 2) Validating the data
- Provided reliable, timely and accurate information;
- Provided efficient access to information by having a centralized web application;
- Provided sustainability of the system by leveraging modern technology;
- Provided a modular system to meet organization growth, changing environment and evolution of client services;
- Enhanced data confidentiality via role based security on user access privileges and provide accountability and
- Standardized system interactions with formal agreements.

The system holds the Official Record of CSE Personnel Security files and National SIGINT Registry information in electronic format, and fulfills the following functions:

- Authorizing special SIGINT compartment indoctrinations and maintaining a national inventory for personnel cleared and indoctrinated to SIGINT as the National SIGINT Registry²;
- Designating “persons permanently bound to secrecy”³;
- Tracking and documenting the processing and results of security clearance screenings of CSE personnel (e.g., employees, contractors, etc.) including storing personal history and incident / investigation information;

² *Policy on Government Security (PGS)*, Treasury Board of Canada Secretariat, 2009-07-01, Appendix B: Communications Security Establishment.

³ *Security of Information Act (SOIA)*.

- Tracking indoctrinations of CSE staff for accesses managed by other organizations, e.g., Department of National Defence (Talent Keyhole/TK), North Atlantic Treaty Organisation (NATO Secret Clearance);
- Storing information to enable the administration of security safeguards of CSE,
- Being the source of record for indoctrination information including de-indoctrinations; and
- Disseminating indoctrination information including de-indoctrinations.

SECTION II – RISK AREA IDENTIFICATION AND CATEGORIZATION

The Levels listed in the last column within each table are treated as INCREMENTAL and CUMULATIVE unless otherwise indicated.

SECTION II - RISK AREA IDENTIFICATION AND CATEGORIZATION

A: Type of System⁴

Level of Risk to Privacy

The information in the system does NOT involve a decision about an identifiable individual

1

The system supports the administration of Programs / Activity and Services

2

Compliance / Regulatory investigations and enforcement

3

Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e.,

Criminal investigation and enforcement / National Security

4

Details:

The system holds the Official Record of CSE Personnel Security information in electronic format, and fulfills the following functions:

- Authorizing special SIGINT compartment indoctrinations and maintaining a national inventory (National SIGINT Registry) for personnel cleared and indoctrinated to SIGINT;
- Authorizing the operation of IT systems and facilities handling SIGINT;
- Designating “persons permanently bound to secrecy”;
- Tracking and documenting the processing and results of security clearances of CSE staff (i.e., employees, contractors, etc.) including storing
- Tracking indoctrinations held by CSE staff for accesses managed by other organizations: i.e. Department of National Defence (Talent Keyhole), North Atlantic Treaty Organisation (NATO Secret Clearance);
- Administrating security safeguards of CSE,
- Functioning as the source of record for indoctrination information including de-indoctrinations; and
- Disseminating indoctrination information including de-indoctrinations.

⁴ Where possible, all references to the “Program or Activity” have been replaced by “System”, as the scope of this PIA is limited to assessing the management of personal information in the SIMON 2.0 application. The Personnel Security Screening program PIA will be a separate exercise, considering the anticipated changes resulting from the upcoming in 2016/2017.

B: Type of Personal Information Involved and Context

Level of risk to
privacy

Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.

1

Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.

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.

3

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.

4

For example: personal information that reveals

Details:

In fulfilling the Security Screening process, personal information that reveals details on financial situation, educational history, criminal history,

C: Program or Activity Partners and Private Sector Access to the SIMON 2.0 System

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

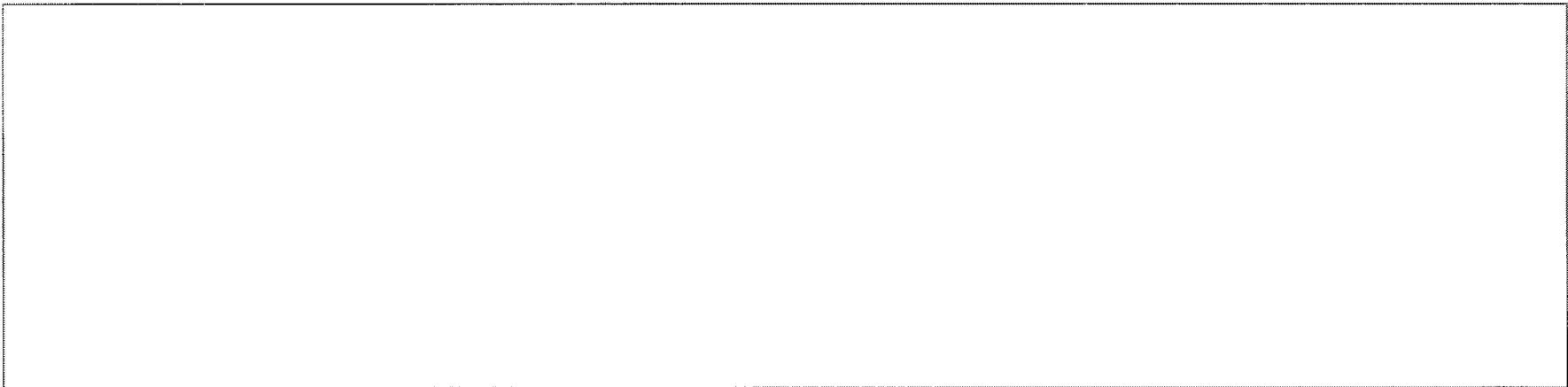
Private sector organizations or international organizations or foreign governments

4

Details:

1. CSE Personnel:

- SIMON 2.0 is accessed by several groups of personnel, including HR, Finance, IT, and Personnel and Physical Security users to track and manage security screenings, physical security and IT security events/infractions, and to access information required to



D: Duration of the SIMON 2.0 System Providing Services to the Physical and Personnel Security Program and the National SIGINT Registry

Level of risk to
privacy

One time program or activity

1

Short-term program

2

Long-term program

3

Existing program that has been modified or is established with no clear "sunset".

Details:

Personnel and Physical Security and the National SIGINT Registry have been established as ongoing programs with no defined end date. CSE owns and manages the Registry, and thus is the authoritative source for indoctrinations for the Government of Canada, providing a service to those federal institutions that own and manage compartmented information.

The SIMON 2.0 system is in place to support the Personnel and Physical Security and National SIGINT Registry programs for the foreseeable future. As with all technology, it is forecast to age out at some point when product support is no longer available; however, this is further in the future than can be predicted at this time, and there no is no clear "sunset".

E: Program Population Reflected within SIMON 2.0

Level of risk to
privacy

- The program affects certain employees for internal administrative purposes.
- The program affects all employees for internal administrative purposes.
- The program affects certain individuals for external administrative purposes.
- The program affects all individuals for external administrative purposes.

1
2
3
4

Details:

The Physical and Personnel Security programs and the National SIGINT Registry affect all employees of CSE, as well as any individuals who apply to work or provide consulting services to CSE. Further, it affects . Data is retained for 5 years if applicants are not subsequently hired/taken on contract, or for a longer period of time (governed by official retention and disposition schedules for data for employees/contractors) if they are successful. Further, the programs affect all government contractors and employees who are indoctrinated to SIGINT Information Access or SIGINT Facility Access.

SIMON 2.0 stores data for all of the individuals affected by the program; therefore, the level of risk has been selected accordingly.

F: Technology and 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?

Certain legacy systems were replaced (SIMON, , OLISS Import, and certain others were not modified; however, the data being supplied to them was drawn from the new SIMON 2.0 database

YES
 NO

3. Does the new or modified program or activity involve the implementation of one or more of the following technologies:

3.1 Enhanced identification methods

Please specify:

YES

[Redacted]

NO

YES

NO

YES

NO

YES

3.2 Use of Surveillance:

Please specify:

Surveillance technologies related to the SIMON 2.0 application are limited to audit trails of all changes to SIMON 2.0 data.

3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

Please specify:

The SIMON 2.0 system does not conduct automated personal information analysis or personal information matching.

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.

Details:

The SIMON 2.0 application supports Corporate Security functions. This upgraded application will replace some legacy systems and will supply other legacy systems with slightly modified data in the same format as they are accustomed to receiving it in order to maintain their functionality. The system will support and enhance the personnel security screening process.

G: Personal Information Transmission

Level of risk to privacy

The personal information is used within a closed system. 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. 3

USB key, diskette, laptop computer, any transfer of the personal information to a different medium.

The personal information is transmitted using wireless technologies. 4

Details:

The personal information stored in SIMON 2.0 is

Full details can be referenced below in Section IV of this PIA.

SIMON 2.0 does not transfer data to portable devices but personal information is printed when required. The application does not provide a specific printing function; however, as it is a web application, the user can use the Mozilla Firefox print feature to print screens. All screens have a dynamic classification up to TS//SI listed on them for inclusion in printed copies.

The specific risk and impact in this category is that

H: Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee

Details:

If there were a breach of confidentiality and privacy and the personal information stored in the system were to be improperly accessed or disclosed to unauthorized users, there would be a potential impact in terms of based on the potential injury to

The assessed level is Disclosure of

Threat rating is PROTECTED B.

I: Potential risk that in the event of a privacy breach, there will be an impact on the institution

Details:

There would be an impact on

Given that the Personnel and Physical Security program and the SIMON 2.0 application are the official source of clearance and indoctrination information relating to SIGNALS Intelligence (SIGINT), there are a few potential scenarios to consider: and

SECTION III – ANALYSIS OF PERSONAL INFORMATION ELEMENTS

SECTION III - ANALYSIS OF PERSONAL INFORMATION ELEMENTS Stored in SIMON 2.0

Personal Information elements and sub-elements

All personal information clusters and elements described below are stored electronically in the SIMON 2.0 database. Physical evidence for these data elements is stored in scanned PDF format in the and referenced within SIMON 2.0 by CERRID # if available.

Personal Information Cluster	Description/Breakdown of Elements (optional)
------------------------------	--

Policy Framework for the Data Elements Stored in SIMON 2.0

CSE follows the requirements described in Appendix B of the TBS *Standard on Security Screening* (“*Security Screening Model and Criteria*”) in its security screening and assessment processes. The following are specifically identified in the *Standard*:

- Identity and background verification
- Educational and professional credential verification
- Personal and Professional reference checks
- Law enforcement inquiry
- Financial inquiry
- CSIS security assessment
- Security questionnaire
- Security interview
- Open Source inquiry
- Polygraph examination

The *Standard for Security Screening* goes on to state that decisions about an individual’s security status or clearance are based on information gathered during the security screening process, that the information is analysed to ensure it is pertinent, authoritative and attributable, and that the context of the position for which the individual is being screened will be taken into account. Negative decisions may be rendered when information is uncovered that raises a reasonable doubt as to an individual’s reliability or loyalty to Canada.

SECTION IV -- FLOW OF PERSONAL INFORMATION

SECTION IV - FLOW OF PERSONAL INFORMATION

The following diagram and tables describe the entities involved in security information related tasks, and the information they exchange currently in SIMON 2.0. SIMON 2.0 will not make significant changes to the basic data flows, but will improve the methods of electronic transmission or remove them altogether as the legacy systems, once accepting transferred data, are integrated.

Legend:

Source of the personal information for the system

Note the original source of all information stored in the SIMON 2.0 system is covered by the Personnel and Physical Security and National SIGINT Registry processes and documentation.

This section has been repurposed to describe how the information is entered into SIMON 2.0.

Input Technique/Source	Description
CSE Personnel Security System User	<p>Can enter any and all personal information elements (described in Section III) stored in the SIMON 2.0 system.</p> <p>This information can come from any source within the program including:</p> <ul style="list-style-type: none"> the individual or representative; a federal government institution;

Internal use and disclosure

Personal Information stored within the Security Information Management and Access Control Systems is circulated with the following systems.

Systems	Description
	<ul style="list-style-type: none"> Internally, basic name, identifying attributes, clearance and indoctrination information is passed to a variety of systems that control access and authentication for the classified network and the Canadian Top Secret Network. In addition, the same information is passed from SIMON 2.0 to the The consumes data from SIMON 2.0 and to identify when people who hold SIGINT Indoctrinations move to a new position, and inform (by an automated email) the indoctrination officer for that compartment in order that they may evaluate whether the person needs to maintain access to that type of information.
Personnel and Physical Security Systems	<ul style="list-style-type: none"> Internally the SIMON 2.0 system transmits data to the . Basic name and identifying attribute information is shared with the to facilitate requests for visitors who do not have a SIGINT indoctrination to visit CSE (especially for the purpose of being screened by Personnel Security). Additionally, an extremely limited amount of information, including the name of the subject and the outcome of their screening request is sent to specific user roles (HR Requestor, Hiring Manager and CP Requestor, and personnel security users) by email sent by SIMON 2.0 via the . These emails are classified as Protected B and managed and protected accordingly. The SIMON 2.0 system stores links to documents containing information

	<p>pertaining to the personnel security file for each individual. Authorized users can employ that link to open the selected documents. In addition SIMON 2.0 retrieves data from electronically in order to send files to and to process</p> <ul style="list-style-type: none"> • Extremely limited identity information for subjects in SIMON 2.0 is electronically transmitted to the system, which attaches identity information to instances of potential security breaches found by the system (• Finally, a copy of the SIMON 2.0 data pertaining to request processing, clearances, indoctrinations, and basic identifying attributes are passed to the database to facilitate quarterly statistical reports, identification of cases with outstanding work, identification of files with anomalous data for cleanup, and to provide in progress reports to HR and Contracting and Procurement to facilitate the hiring/contracting process. Access to this database is restricted according to CSE database management policies, and information in the database is therefore, the retention period for this database is • Internally SIMON 2.0 electronically transmits the name, basic identifying attributes and clearance and indoctrination information to the system in order to facilitate the evaluation and processing of visit requests from CSE visitors going to
--	---

Internal Transmission and Disclosure of Detailed Data Elements

This table describes the data elements which are electronically transmitted from the SIMON 2.0 system to another system.

Data Grouping	Data Elements							
Name		Y		Y		Y	Y	Y
		Y	Y	Y		Y	Y	Y
		Y				Y		Y
						Y		Y
			Y					Y
		Y	Y					Y
			Y					Y
			Y					Y
Attributes		Y	Y			Y		Y
			Y			Y		Y
		Y	Y	Y	Y	Y	Y	Y
		Y				Y	Y	Y
		Y		Y		Y	Y	Y
		Y	Y	Y		Y	Y	Y
		Y				Y		Y
		Y				Y		Y
		Y	Y	Y		Y		Y
		Y				Y	Y	Y
		Y		Y		Y		Y
		Y						Y
		Y						Y

Data Grouping	Data Elements						
							Y
		Y			Y	Y	
		Y					Y
		Y					Y
		Y					Y
			Y				Y
			Y				Y
					Y		Y
					Y		Y
					Y	Y	Y
		Y	Y		Y	Y	Y
						Y	Y
							Y
		Y	Y	Y		Y	Y
		Y					Y
		Y					Y
		Y		Y			Y
		Y			Y		Y
				Y			Y
							Y
		Y	Y				Y
							Y
		Y	Y				Y
							Y
		Y			Y	Y	Y
		Y					Y

Data Grouping	Data Elements
Email Notification	
ALL DATA	

External Transmission and Disclosure

The Individual or Representative	n/a
Another Federal Government Institution	<p style="text-align: center;">will receive information from CSE related to the Personnel and Physical Security Program and/or the National SIGINT Registry. In addition,</p>

	<p>The Public Works and Government Services Canada, 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: RCMP, Security/Reliability Screening Records - RCMP PPU 065; CSIS, Security Assessments/Advice - CSIS PPU 005. 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.</p> <p>The CSE Personnel Security Office maintains a list of all GC employees who are indoctrinated for access to special information (SI) SIGINT and related within SIMON 2.0. A view of the required data (name, DOB, citizenship, clearance, indoctrination, status) for the CTSN version is provided within the SIMON 2.0 database. The view is used to upload the data to the CTSN and it is made available on the CTSN site. Those indoctrinated for access to SIGINT/TK/GAMMA and who have access to CTSN can therefore verify which other GC employees have up to the same level of indoctrination are not made visible within CTSN</p> <p>In addition, CTSN utilizes identity, clearance, and indoctrination information to provision access to the CTSN network.</p>
--	---

Non-federal institutions and private sector	
Provincial Government	N/A
Municipal Government	N/A
Aboriginal Government/ Council	N/A
International Organization	
Private Sector	
Located in Canada and Canadian Owned	N/A
Located in Canada and Foreign Owned	N/A
Located abroad and Canadian Owned	N/A

--	--

Retention / Storage

A Federal Government Institution	CSE Data Centre – all data stored within the SIMON 2.0 application
A Federal Records Center	Not applicable. Personnel and Physical Security records are not transferred to Library and Archives Canada or retained at any federal records centre. Documents are disposed at CSE according to the retention and disposition policy.
Non-federal institutions and private sector	
Provincial Government	N/A
Municipal Government	N/A
Aboriginal Government/ Council	N/A
Organization of a Foreign State	N/A
International Organization	N/A
Private Sector	
Located in Canada and Canadian Owned	N/A
Located in Canada and Foreign Owned	N/A
Located abroad and Canadian Owned	N/A
Located abroad and Foreign Owned	N/A

OTHER POSSIBLE CONSIDERATIONS

The following table identifies the areas / groups / divisions who are allowed to access and handle the personal information stored within the SIMON 2.0 system (or as a direct result of receiving information from the SIMON 2.0 system).

Federal Government Institution who have primary access to the data within the system:		
Identify Groups or Areas / or Divisions	Where appropriate - positions who have access or use the personal information	Geographical Location
CSE Corporate Security – Personnel and Physical	Staff of approx. individuals – Security Officers and related personnel.	National Capital Region
CSE Desktop Services (CIO)	Desktop Services have access to name, DOB, Place of birth, clearance and indoctrination information to facilitate providing hardware and software services	National Capital Region

	to authorized individuals.	
CSE staff and contractors	To request an update to their own personal information only and to confirm indoctrination levels of others to their own level.	National Capital Region
Other federal government Institution who [redacted]		from the system:
		National Capital Region
Other federal government institutions who [redacted]		from the system:
		National Capital Region
		National Capital Area – specifically 1929 Ogilvie Road, Gloucester, Ottawa

SECTION V – PRIVACY COMPLIANCE ANALYSIS

SECTION V - PRIVACY COMPLIANCE ANALYSIS

LEGAL AUTHORITY FOR THE STORAGE⁵ OF PERSONAL INFORMATION

1. Has a legal authority been identified for the storage of personal information in the SIMON 2.0 System?

⁵ Where possible, all references to “collection” in Section V have been replaced by “storage”, as we are assessing SIMON 2.0 in its role as the official CSE repository of personnel security-related personal information (which is actually collected by the Personnel Security, Physical Security and National SIGINT Registry programs).

YES

Please specify the legal authority and briefly explain how it permits the storage of the personal information in the SIMON 2.0 system:

The *Library and Archives of Canada Act* governs the management of information within the Government of Canada, including the management of personnel security screening information contained in the SIMON 2.0 repository.

Section 7.1 of the *Financial Administration Act (FAA)* provides CSE the overall legal authority to collect information for the purposes of personnel security screening under the Personnel and Physical Security programs. The *National Defence Act (NDA)*, *Security of Information Act (SOIA)* and the *CSSS-100: SIGINT Protection and Control* policy authorize the collection of indoctrination information for the purposes of managing the National SIGINT Registry.

AND, ensure that the legal authority to store the personal information is cited in the relevant PIB (See the Executive Summary)

Continue to Question 2

NO

If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your institution's legal advisors to determine if there is authority to proceed with the program or activity.

NECESSITY TO COLLECT PERSONAL INFORMATION

Please note that this section is not relevant to the PIA from a systems perspective, as the SIMON 2.0 does not collect the personal information. The system is simply a repository for the personal information (which is actually collected by the programs).

2. Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

AUTHORITY FOR THE COLLECTION, USE OR DISCLOSURE OF THE SOCIAL INSURANCE NUMBER

Please note that this section is not relevant to the PIA from a systems perspective, as SIMON 2.0 is simply a repository for the information (which is actually collected by the program). However, we confirm that the SIN is not collected by the program, nor is it stored in the system.

3. Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

NO

The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

DIRECT COLLECTION – NOTIFICATION AND CONSENT, AS APPROPRIATE

Please note that this section is not relevant to the PIA from a systems perspective, as SIMON 2.0 is simply a repository for the information. The collection of the personal information is performed by the Personnel and Physical Security programs.

4. Is personal information collected directly from the individual to whom it relates?

- Notification and informed consent are provided to the individual as part of the administration of the programs (i.e., individuals are required to complete the *Personnel Screening, Consent and Authorization Form* TBS-330-23 and *Security Clearance Form* TBS 330-60 at the point of collection, both of which contain appropriate privacy notice statements.) The SIGINT Indoctrination, De-Indoctrination, and Exit Interview forms also contain appropriate privacy notice statements. The PNSs on these forms meet all of the requirements in listed in section 4, below.

The program-level PIA will provide the complete privacy analysis.

INDIRECT COLLECTION - CONSENT OR AUTHORITY PURSUANT TO SECTION 10 OF *PRIVACY REGULATIONS*

Please note that this section is not relevant to the PIA from a systems perspective, as the system is simply a repository for the information (which is actually collected by the program).

5. Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the *Privacy Regulations*?

NO



NOTE: From a program perspective, the information collected for the security screening process is completely driven by the *Personnel Screening, Consent and Authorization* form (TBS-330-23), which is very inclusive. If additional information outside of its stated purpose is needed, Personnel Security Officers list the consistent uses under "OTHER" and get a signature from the subject for permission.

INDIRECT COLLECTION - WITHOUT NOTIFICATION AND CONSENT

Please note that this section is not relevant to the PIA from a systems perspective, as the system is simply a repository for the information (which is actually collected by the program).

6. Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

NO

All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above).

RELEVANT PRIVACY NOTICES

As this PIA relates to the implementation of the SIMON 2.0 system, which is a repository for data collected by the Personnel and Physical Security Program and the National SIGINT Registry Program, currently, there is no Privacy Notice Statement.

We have chosen to include the SIMON 2.0 Notice on the login screen to demonstrate that SIMON 2.0 users are alerted every time they access the system as to the importance of handling the data in an appropriate manner and the consequences of unauthorized use and disclosure.

SIMON 2.0 Notice on Login Screen

All users logging on to the SIMON 2.0 application are presented with the message below.

SIMON 2.0 (Security Information Managed Online)

The Security Information Managed Online system "SIMON 2.0" is CSE's personnel security information electronic database and also serves as the National SIGINT Registry. SIMON 2.0 contains personal data pertaining to CSE applicants, contractors, employees, students, secondees, integrees and other Government of Canada (GoC) employees and contractors who may hold SIGINT indoctrination. This information held is used to facilitate the screening, clearance processing and recording of clearance/indoctrinations/de-indoctrination status and security violations pertaining to GoC personnel. Data within this system may be sourced from and shared with other departments and organizations in compliance with authorized derivative use purposes. Unauthorized access to this system is strictly prohibited.

The SIMON 2.0 system is to be accessed in the conduct of the employee's duties and only in the manner authorized by CSE's policies. All activities on the system are subject to be monitored and audited by CSE. Monitoring of CSE systems is performed by authorized personnel and reported to CSE management. The use of the SIMON 2.0 computer system, authorized or unauthorized, constitutes consent to monitoring on this system.

Non-compliance with CSE's policies including unauthorized disclosure of information to third parties may result in disciplinary actions.

By logging in, you acknowledge that you have read and understood the terms and conditions of using this application.

Retention and Disposal of Personal Information

RETENTION AND DISPOSAL OF PERSONAL INFORMATION IN SIMON 2.0

Please note that this section is not structured in a relevant manner for the PIA from a systems perspective, as the system is simply a repository for the information (which is actually collected by the programs).

However, it should be noted that Library and Archives Canada has authorized retention schedules for personal information collected by the programs:

- The RDA for Corporate Security Activities is 97/003. Employee and Contractor and Student Security files are retained for DoB +80 yrs, or 15 years after the last administrative action, whichever is later;
- Applicant Security Files are retained for 5 years from the screening completion date, or 2 years after the last administrative action, whichever is later.
- Polygraph files are retained for 5 years from the last polygraph date. Psychological Assessment Files are retained for 5 years after the last psychological assessment date.

The SIMON 2.0 system addresses the requirement for appropriate retention and disposal of personal information by having a reporting functionality to identify records due for disposal, and an electronic disposition function which deletes data that are beyond their retention date once all policies and procedures have been applied.

7. Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

YES

**ACCURACY OF PERSONAL INFORMATION RETAINED IN SIMON 2.0**

Please note that this section has been answered from the perspective of the system. The specific actions that program officials use to ensure accuracy of the personal information in SIMON 2.0 are outlined in section 8, below.

8. Will all reasonable measures be adopted to ensure that personal information (stored in SIMON 2.0) used by the institution for an administrative purpose is as accurate, up-to-date and complete as possible?

YES

Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.

Although the subject individual does not enter the data into the SIMON 2.0 system, wherever possible, it is collected from them directly, either by paper (i.e., through the TBS Personnel Security Screening forms, or electronically through another system.) The program officials ensure that individuals are given the opportunity to validate their data at the original point of collection and during the security clearance update period.

In cases where direct collection or consent is not feasible, the institution will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use. Please identify the sources and procedures to be used to check the accuracy of the information:

Bearing in mind that the SIMON 2.0 application does not collect information directly from the individual; nonetheless, when data is gathered and is entered into the SIMON 2.0 application, in certain circumstances, it will have been obtained from trusted sources instead of the individual

and the accuracy will be verified prior to input.

For example:

- CSE obtains information directly related to the standard screening process from trusted government sources (e.g.,
 - i.
- Credit Check information is obtained from _____ and is verified by the individual through _____ provided by the individual and reviewed at the Subject Interview.
- Occasionally employment and character references supplied by the subject will be contacted as part of the screening process.
 - o The information acquired, as well as all data on the Security Clearance Form is likewise reviewed with the individual during the Subject interview process and subsequent follow-up interviews and phone calls.

USE OF PERSONAL INFORMATION

Please note that this section is not structured in a relevant manner for the SIMON 2.0 PIA from a systems perspective, as the system is simply a repository for the information (which is actually collected and used by the program). The analysis of s. 8(2) uses will be outlined in the program-level PIA.

9. Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of Privacy Act

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of Directive on Privacy Practices, section 6.2.15 of

Policy on Privacy Protection and Section IV of Appendix C of Directive on Privacy Impact Assessment

Note that the personal information is not accessed, shared, or disclosed for non-administrative purposes.

DISCLOSURES DIRECTLY RELATED TO THE ADMINISTRATION OF THE PROGRAM OR ACTIVITY VIA SIMON 2.0

Note that these questions are being answered from the perspective of the SIMON 2.0 system, not the program. The responses identify what data stored in the system is shared via user access to the system or electronic transmission to other systems, regardless of whether it is directly or indirectly related to the program.

10. Will personal information be disclosed for purposes directly related to the administration of the program or activity?

YES

Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the institution or with other federal government institutions, please identify the branch and the program or activity.

Within the institution for another program or activity – specify

Screening level, Clearance Level, and Indoctrination status is shared along with name to the _____ Clearance and Indoctrination Level is shared with SIMON 2.0 users who have equivalent indoctrinations.

With programs or activities of other federal government institutions – specify

The following are the scenarios in which other federal government institutions or systems receive information from SIMON 2.0:

Provincial, territorial or municipal governments institutions – specify

Foreign government institutions and entities thereof – specify

Authorized employees/contractors of

to see a list of other users with equivalent

indoctrinations.

International organizations – specify

The private sector (e.g., contractor or other external service provider) – specify

Other – specify

AND, ensure that:

a) any such disclosure is made in compliance with the program or activity enabling legislation or section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;

b) only personal information elements that are necessary for the intended purpose are disclosed;

c) the organization or third party receiving the personal information is authorized to do so;

- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant PIB in *Info Source*, including the specific purpose of the disclosure;
- f) the "Privacy Notice" or "Consent Statement" describes any disclosures of information; and,
- g) the "Data Flow Diagram" or "Data Flow Tables" completed in "Section IV – Flow of Personal Information" of the core PIA include details on the disclosed personal information: (See Section IV of Appendix "C" of Directive on Privacy Impact Assessment for a list of elements that must be included in the data flow diagram or data flow tables.)

AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement:

See SECTION VII – Supplementary Documents List for a complete list of relevant contracts, MOUs and Agreements.

ACCOUNTING FOR NEW USES OR DISCLOSURES NOT REPORTED IN INFO SOURCE

Please note that this section is not structured in a relevant manner for the PIA from a systems perspective, as the system is simply a repository for the information (which is actually collected by the programs). This will be assessed by the program level PIA.

11. Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in *Info Source*? **Statutory reference:** Sections 7 to 11 of *Privacy Act* and section 4 of *Privacy Regulations*
Policy reference: Sections 6.1.9 and 6.2.2 of *Directive on Privacy Practices*

SAFEGUARDS - STATEMENT OF SENSITIVITY

Please note that we are answering this section from the perspective of the system, not the program, however we confirm that a Statement of Sensitivity has been completed.

12. Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

YES

The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section II - Risk Area Identification and Categorization" of the core PIA:

- *SIMON 2.0 Statement of Sensitivity* (CERRID # 11115448)

SAFEGUARDS – THREAT AND RISK ASSESSMENT

Please note that we are answering this section from the perspective of the system, not the program.

13. Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity?

NO

If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain why not.

CIO has determined that a formal TRA is not required for SIMON 2.0; however, a thorough assessment of the risks, security controls and procedures has been completed as part of the Security Accreditation and Assurance process implemented by CSE to ensure all systems implemented at CSE are secured (CERRID Folder # 8870327). The body of evidence created by CIO as part of this process includes a Statement of Sensitivity, CONOP,

SAFEGUARDS – ADMINISTRATIVE, PHYSICAL AND TECHNICAL

Please note that we are answering this section from the perspective of the system, not the program.

14. Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Administrative safeguards

- Internal security and privacy policies and procedures
- Staff training on privacy and the protection of personal information
- Screening and security checks of employees
- Appropriate security levels for employees who will have access to personal information
- Contingency plans and documented procedures in place to identify and respond to security and privacy breaches
- Regular monitoring of users' security practices
- Methods to ensure that only authorized personnel who need to know have access to personal information
- Other – please describe

- and audit logs
- thereof.
- Contingency plans and procedures are in place to identify and respond to security breaches.
- Specific privacy obligations for the use of the SIMON 2.0 system are outlined in the *SIMON 2.0 User Access Agreement – Terms and Conditions* (Cerrid #27178935)
- Policies (*ORG-6-1*) and procedures for responding to privacy breaches are in place at the institutional level.

Physical safeguards

Technical safeguards

TECHNOLOGY AND PRIVACY - TRACKING TECHNOLOGIES USED BY SIMON 2.0

Please note that we are answering this section from the perspective of the system, not the program.

15. Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

YES

The specific tracking technologies to be used are described under Part F: Technology and Privacy of "Section II – Risk Area Identification and Categorization" of the core PIA

AND, the collection of any personal information using such technologies is reflected in the relevant PIB and in "Section III – Analysis of Personal Information Elements" of the core PIA;

AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice":

- Users of the system receive an on-screen message agreeing to the terms of use for the Secured Network Usage – Network Usage Policy, they receive orientation training materials, and core users of the SIMON 2.0 system sign a *SIMON 2.0 User Access Agreement Terms and Conditions of Use* when they receive a Privacy Briefing.

AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;

AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the Privacy Regulations.

TECHNOLOGY AND PRIVACY – SURVEILLANCE OR MONITORING

Please note that we are answering this section from the perspective of the system, not the program.

16. Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

NO

The upgraded system will not result in new or increased surveillance or monitoring. The system supports an existing program/activity.

PRIVACY CONSIDERATIONS RELATED TO COMPLIANCE / REGULATORY INVESTIGATION AND ENFORCEMENT

Neither the program nor the system conducts any activities relevant to this section.

17. Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

NO

The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

Note that while in Section 2 we have selected risk level regarding Compliance/ Regulatory investigation and Enforcement, this is limited to and therefore does not appear to be covered under this Privacy Compliance Section. The Personnel and Physical Security Programs do not conduct criminal investigations or enforcement activities.

SECTION VI - SUMMARY OF ANALYSIS AND RECOMMENDATIONS

SECTION VI - Summary of Analysis and Recommendations (as applicable) Document the conclusion drawn or recommendations resulting from the risk identification and categorization in a manner that

is commensurate with the risk identified.

Overview of the Analysis and Recommendations:

The SIMON 2.0 system contains personal information in accordance with s. 3 of the *Privacy Act*. The information stored in the system is used by the Personnel and Physical Security programs to conduct personnel security screening. As such, the uses are described and governed within the standard TBS PIB, PSU 917 (Personnel Security Screening). Information stored within SIMON 2.0 accessed and disclosed in accordance with uses and disclosures listed within the Personnel Security Screening PSU 917.

Internal Transmission/Disclosure:

Personal Information is shared with systems within the CSE Classified network for the purpose of controlling access to physical, information, and technical resources

It is also shared with systems inside the CSE Classified network for the purpose of maintaining information relevant to the subject's personnel security file, including managing access to scanned personnel security file documents in CERRID (CSE's corporate records management system), reviewing and for the conduct and tracking of related to the subject.

External Transmission/Receipt/Disclosure

Personal information related to security screening is securely received from the OLISS application maintained by PSPC (previously PWGSC) and imported into the SIMON 2.0 system. Information related to TK indoctrinations is securely received from DND and imported into the SIMON 2.0 system.

Information is securely and directly transmitted to the network for the purpose of controlling access to information and technical resources. In addition, information is securely and directly transmitted to systems to facilitate the security screening process.

Access and use of the personal information contained in SIMON 2.0 by is limited and controlled. For details on how SIMON 2.0 data is transmitted to others systems, see the Data Flow Diagram at the beginning of section IV.

Staff who are onsite may also directly access information from the SIMON 2.0 system related to confirming that other individuals hold the same level of indoctrinations as themselves.

All of these uses for the personal information stored within SIMON 2.0 are consistent with the stated purpose of the PIB and represent an acceptable risk level provided that the information is adequately managed and protected.

Finally, in support of the National SIGINT Registry program, information related to indoctrination levels held by CSE employees, GoC employees who have access to SIGINT is recorded, accessed, used, updated, maintained, transmitted, and disposed of by SIMON 2.0.

In general the risk level of the SIMON 2.0 system is rated risk level for each category is listed below:

A summary of the assessed

Risk Category	Descriptive Risk Level	Assessed Risk Level
Type of System	Compliance / Regulatory investigations and enforcement	
Type of Personal Information Involved and Context		
Program or Activity Partners and Private Sector Involvement		
Duration of the Program or Activity	Long-term program	
Program Population		
Technology and Privacy	Implementation of a new electronic system requires modifications to IT legacy systems and / or services. <u>Implementation involves:</u> b) Use of Surveillance (audit logs)	
Personal Information Transmission	The personal information is	
Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee		
Potential risk that in the event of a privacy breach, there will be an impact on the institution		

In general, the system contains data which is designated Protected B and the risk to individuals in the event of a compromise is commensurate with that; however, the risk to CSE in the event of a compromise could be

The system has been classified that were a user to

to reflect the fact the risk would be rated at

Recommendations:

Given the nature of the personal information collected, the risk represented by the following recommendations are being made to ensure that the personal information in the SIMON 2.0 system is adequately protected:

- Ensure adequate technical safeguards are in place to safely protect information stored within the system; for example,
- Ensure that the data in the SIMON 2.0 system is protected by
- Ensure that in order to access SIMON 2.0 data and that for the intended purpose;
- Ensure that restricting those users who can access the data provided by SIMON 2.0 to those who are authorized and have an identified business purpose consistent with the PIB under which the data was collected;
- Ensure that edits, updates, and deletes of data from the SIMON 2.0 system are audited and integrated into audit analysis software;
- Ensure that personnel who have access to the SIMON 2.0 system are adequately trained with regards to Privacy principles and obligations, and that the training is refreshed on a periodic basis;
- Ensure that the PIAs for downstream systems controlled by CSE (CERRID) are complete; and
- Ensure that an adequate assessment of the security threats and risks to the system is completed and that its recommendations are implemented to ensure the security of data.

Mitigation:

Recommendation	Mitigation
1. Ensure adequate technical safeguards are in place to safely protect information stored within the system. <ul style="list-style-type: none"> • For example, ensure that the system 	CIO ensures any system that has been properly vetted. Each layer of the has been accredited by CIO's SA&A process which include:
2. Ensure that the data in the SIMON 2.0 system is protected by	SIMON 2.0's security model restricts and controls access based on . The security model extends beyond SIMON 2.0 the application and also includes CSE's which including SIMON 2.0.
3. Ensure that in order to access SIMON 2.0 data, and that	Access to SIMON 2.0 is based on what information each

<p>for the intended purpose.</p>	<p>system requires, and insure data integrity. are put in place to SIMON 2.0 audit keeps a record of which individuals, and which system access SIMON 2.0 data.</p>
<p>4. Ensure that restricting those users who can access the data provided by SIMON 2.0 to ONLY those who are authorized and have an identified business purpose consistent with the PIB under which the data was collected.</p>	<p>The information is restricted based on pre-approved access by are put in place to ensure only approved data is shared with And access to the is further restricted by</p> <p>Regular audits of existing and new users are completed to ensure that only individuals with a legitimate business need to access SIMON 2.0 may do so. Once an individual moves to a role which no longer requires access to the system, the individual's account and access privileges are deleted.</p>
<p>5. Ensure that edits, updates, and deletes of data from the SIMON 2.0 system are audited and integrated into audit analysis software.</p>	<p>SIMON 2.0 keeps detailed audit logs that capture edits, updates, and deletes of information. The SIMON 2.0 audit logs are also provided to IT security for further analysis and monitoring. CSE Corporate Security Directorate is in the process of establishing a to monitor the use of the system, including abuse of access privilege.</p>
<p>6. Ensure that Privacy Impact Assessments for downstream systems controlled by CSE (e.g., CERRiD) are completed; and</p>	<p>CIO has been working diligently to ensure steps are taken to have all systems that are PIA candidates to undergo a privacy impact assessment review.</p>
<p>7. Ensure that an adequate assessment of the security threats and risks to the system is completed and that its recommendations are implemented to ensure the security of data.</p>	<p>CIO is responsible for assessing the SIMON 2.0 application and hardware. Accordingly, the Security Assessment and Accreditation process (CERRiD Folder #8870327) has provided SIMON 2.0 with Authority to Operate based on the technical assessment and the acceptance of residual risk.</p> <p>All new threats/risks identified by CIO will be addressed to the satisfaction of the assessor, and approved by both CIO and the application owner, Corporate and Physical Security.</p>
<p>8. Ensure administrative safeguards are in place to safeguard the privacy and confidentiality of the information in the system.</p> <p>Ensure that personnel who have access to the SIMON 2.0 system are adequately trained with regards to Privacy principles and obligations, and that the training is refreshed on a periodic base.</p>	<p>All CSD employees receive ongoing training on privacy and security.</p> <p>have implemented a new SIMON 2.0 User Access Terms and Conditions Agreement (CERRiD #27178935). provides a mandatory briefing to inform new and existing users of their privacy obligations prior to assigning (or renewing) user access to the system.</p> <p>Retention and disposition schedules are implemented to manage PI that has met its life-cycle. Routine purges of information in SIMON 2.0 are performed by , in collaboration with CIO (responsible for managing and disposing the hard-copy records).</p>

SECTION VII – SUPPLEMENTARY DOCUMENTS LIST

Project and Product Scope Reference Documents and Policies

- SIMON 2.0 Project Charter CSE CERRID # 14758250
- SIMON CONOPS CSE CERRID # 10588508
- Functional Requirements Matrix CERRID #270292
- Functional Requirement Definition Report CERRID #270289
- SIMON Business Architecture Components for Clearance, Indoctrination and Comp Management (Titled SIMS – business architecture deliverables– CERRID #824565
- SIMON Program overview CERRID #212549

Business Requirements Reference Documents and Policies

- SIMON Business Architecture CSE CERRID #853161
- SIMON – Screening Module Functional Design Section 1 – Initial Processing #18169286
- SIMON – Screening Module Functional Design Section 2 – Subject Interview #21256615
- SIMON – Screening Module Functional Design Section 3 – End Process #22716486
- SIMON – Subject Management Module Functional Design #22123160

Risk Assessments and Risk Management

- **SIMON Security Accreditation and Assurance (SA&A) Process folder CERRID # 8870327**
- SIMON Statement of Sensitivity Profile CSE CERRID #11115448
- SIMON – System Architecture Document CERRID # 18824250
- SIMON - Role Based Security Screen and Function Level CERRID-#900341

SIMON Training, Quick Reference Guides and User Manual

- SIMON 2.0 Training Folder CERRID #8850964
- SIMON Guides Folder CERRID #8986609

Contracts / Memoranda of Understanding / Agreements

- *SIMON 2.0 User Access Agreement Terms and Conditions* CERRID #27178935

SECTION VIII – APPROVAL

SECTION VIII A – Program-Level Approval

I have reviewed, and recommend the approval of this Core PIA, and commit to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements as they relate to the administration of SIMON 2.0.

Director, Corporate Security Directorate

[Signature Box]

Signature / Date

SECTION VIII B – LEGISLATIVE APPROVAL UNDER THE *PRIVACY ACT*

The Official who has immediate jurisdiction over the SIMON 2.0 Program and System is: the Director General, Corporate Services Operations

I approve of this Core PIA and commit to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements as they relate to the administration of SIMON 2.0.

Director General, Corporate Services Operations
Departmental Security Officer

Michel Komery

[Signature] / Date
23 Mar 2017

The Delegated Heads of the CSE ATIP Program, responsible for administering section 10 of the *Privacy Act* are the Director, Disclosure Policy and Review, and Deputy Chief, Policy and Communications CSE:

I approve this Core PIA and am satisfied that it complies with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements as they relate to the administration of the SIMON 2.0 system.

Director, Disclosure Policy and Review

Nabih Eldebs

[Signature] / Date
28 Mar 2017

Deputy Chief, Policy and Communications,
Chief Privacy Officer

Dominic Rochon

[Signature] / Date
28 Mar 2017

SECTION IX – APPENDICES

APPENDIX A - GLOSSARY OF TERMS AND ACRONYMS**Information Context**

Information	Description
SIMON 2.0	Security Information Managed Online Version 2.0
National SIGINT Registry	National Registry of Personnel cleared and indoctrinated in SIGINT
Official record	Record of decisions, events and other comprise the official record of the CSE Personnel Security function
SIGINT	Signals Intelligence
	- SIGINT

Acronyms

Acronym	Description
CIO	Chief Information Office
COMSEC	Communications Security (name of a program which assists in the protection of classified information and data)
CSA	Construction Site Access
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CSOPS	Corporate Services Operations
CTSN	Canadian Top Secret Network (formerly known as Mandrake; a GC Top Secret level network for the sharing of intelligence information)
DND	Department of National Defense

MANDRAKE	Mandrake - now CTSN – former name of the GC Top Secret Intelligence Network
MOU	Memorandum of Understanding
OLISS	On-Line Industrial Security Services
PHF	Personal History Form (now called Security Clearance Form)
PM	Project Manager
PSC	Project Steering Committee
PWGSC / PSPC	Public Works and Government Services Canada (now Public Services and Procurement Canada)
RCMP	Royal Canadian Mountain Police
SCF	Security Clearance Form (previously known as Personal History Form)
SFA	SIGINT Facility access (formerly known as SIGINT Site Access)
SIGINT	Signals Intelligence
SIA	SIGINT Information Access
SIMON	Security Information Managed Online application
SLA	Service Level Agreement
SOIA	Security of Information Act
SSA	SIGINT site access (now known as SIGINT Facility Access)
WBS	Work Breakdown Structure

**CORE PRIVACY IMPACT
ASSESSMENT FOR:**

Applicant Tracking System

**CSEC-CSTC
CSSEC / CIO / CIO**

CERRID ID #24981335

Change Control Table

Version	Date	Change Made By	Change Requested By	Change
1.0	Oct 6, 2014	CIO		New document
2.0	Jan 16, 2015	CIO		Update data descriptions.
3.0	Jan 27, 2015	CIO		Updates incorporating feedback from
4.0	Jan 29, 2015	CIO		Add "Description of Program or Activity" and "Legal Authority for Program/Activity" content.

Table of Contents

SECTION I - RISK AREA IDENTIFICATION AND CATEGORIZATION 3

SECTION II - ANALYSIS OF PERSONAL INFORMATION ELEMENTS 9

SECTION III - FLOW OF PERSONAL INFORMATION 11

SECTION IV - PRIVACY COMPLIANCE ANALYSIS..... 12

SECTION V - SUMMARY OF ANALYSIS AND RECOMMENDATIONS (AS APPLICABLE)..... 29

SECTION VI - SUPPLEMENTARY DOCUMENTS LIST..... 31

SECTION VIII – FORMAL APPROVAL 32

SECTION I - RISK AREA IDENTIFICATION AND CATEGORIZATION

A: <u>Type of Program or Activity</u>	Level of Risk to Privacy
Program or activity that does NOT involve a decision about an identifiable individual	<input type="checkbox"/> 1
Administration of Programs / Activity and Services	<input checked="" type="checkbox"/> 2
Compliance / Regulatory investigations and enforcement	<input type="checkbox"/> 3
Criminal investigation and enforcement / National Security	<input type="checkbox"/> 4

Details:

The Applicant Tracking System (ATS) is a service enhancement for CSE external website. The purpose of the ATS tool is to facilitate external hiring for CSE. External applicants are asked to go into the system and submit a resume and answer various questions. All external applicants (including students) must use the system to apply as only those applications coming through the system will be considered for employment.

The web component of the Applicant Tracking System (ATS) will be hosted on CSE external web server (DMZ server), offering the new interface to job applicants and the CSE HR staffing advisors with a content publisher role. The new system will enforce proper security features to protect applicant data.

The ATS site was developed using [redacted] as a Content Management System (CMS). The CMS allows granting a content publisher role to a HR staff. However, the HR content publishers need to follow a formal procedure on the content approval and translation. The applicant will be able to apply for a specific position using an online form accessible from the Careers section on CSE external website. An applicant's resume and cover letter will be included into the application form using the copy or paste function. Submitted job applications are stored temporarily in the webserver database. Database submissions are downloaded daily (5 days per week) by the web team. The output file is generated in XML format and saved on a [redacted] system. The web database will be purged daily to minimize data retention on external server in order to meet CSE security requirements. The CSE web team will download XML file [redacted] and delete it after a successful transfer to [redacted] network. The applicant data received from the external website will be automatically scanned [redacted] before uploading to [redacted] network. On [redacted] network the custom script will process the XML file and upload to PeopleSoft. The HR staffing advisors will access PeopleSoft application on secure network to process applicant data.

The proposed Applicant Tracking System will replace the existing web-based recruitment system, an application hosted by [redacted]. The existing contract with [redacted] was extended (in fall 2014) until 31 of March, 2016, however the [redacted] site will only be used up to March 2016 to access historical data.

This initiative is an IM/IT priority as it was approved by the IM/IT steering committee for this fiscal.

The new system will allow CSE to have full control over collected data, improving the privacy and protection of the applicant's information.

Why is there a need and who approved the need?

Due to a nature of our organisation the new system is required to offer full control over data of people applying for positions at CSE to protect their identity

B: Type of Personal Information Involved and Context

Level of risk to privacy

Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.

1

Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.

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.

3

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.

4

Details:

ATS collects Application for Employment (PIB Bank No. PSU-911) and contact information directly from Internet based end-users as potential candidates for internal positions.

Application for Employment

Description: This bank describes personal information related to individuals who have submitted applications for employment or provided curricula vitae (solicited or unsolicited) and related correspondence. The personal information provided by individuals on application forms, curricula vitae, and correspondence may include: name, contact information, employment status and history, educational background, marital status, date of birth, gender, official language proficiency, employment equity, physical disability considerations, citizenship, Personal Record Identifier, Client Server Number, transcripts, letters of recommendation, and other personal information.

Class of Individuals: Public service employees and non-public service employees seeking employment with the institution; individuals whose names have been provided as employment references, personal references, or both; and individuals referring another individual for a position.

Purpose: To maintain an inventory of potential candidates that may be used for consideration in a staffing process when vacancies arise within the institution.

Consistent Uses: Relevant information would be transferred to an employee personnel record (refer to Standard Personal Information Bank Employee Personnel Record – PSE 901) if the individual accepts an offer of employment. This information may also be used for planning and evaluation purposes. The information may also be transferred to another institution, if the other institution is deemed to be more appropriate for potential employment opportunities for the individual. The data collected and maintained may be used for statistical purposes, training requirements, and other development opportunities. The personal information about individuals self-identified in employment equity groups may be used for statistical purposes by the institution and may be shared with the Public Service Commission of Canada, Treasury Board of Canada Secretariat, and Canada Public Service Agency for the same purpose.

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: 98/005

Related Record Number: PRN 920

Bank Number: PSU 911

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

Details:

ATS collects Application for Employment (PIB Bank No. PSU-911) and contact information directly from Internet based end-users for the purposes of evaluating potential candidates for internal CSE positions. In some cases, the applicant information may be shared with other federal institutions as potential candidates for positions within that institution, subject to applicant’s consent.¹

¹ The disclosure process is outside the scope of the ATS project and is not covered by the ATS PIA.

D: <u>Duration of the Program or Activity</u>	Level of risk to privacy
One time program or activity	<input type="checkbox"/> 1
Short-term program	<input type="checkbox"/> 2
Long-term program	<input checked="" type="checkbox"/> 3
<u>Details:</u> Applicant Tracking System is an HR application that will likely be in operation for the long-term.	

E: <u>Program Population</u>	Level of risk to privacy
The program affects certain employees for internal administrative purposes.	<input type="checkbox"/> 1
The program affects all employees for internal administrative purposes.	<input type="checkbox"/> 2
The program affects certain individuals for external administrative purposes.	<input checked="" type="checkbox"/> 3
The program affects all individuals for external administrative purposes.	<input type="checkbox"/> 4
<u>Details:</u> ATS collects Application for Employment (PIB Bank No. PSU-911) and contact information from Internet based end-users as potential candidates for internal positions.	

F: <u>Technology and Privacy</u>	
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?	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
2. Does the new or modified program or activity require any modifications to IT legacy systems and / or services?	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
3. Does the new or modified program or activity involve the implementation of one or more of the following technologies:	
3.1 Enhanced identification methods	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
Please specify:	
<input style="width: 600px; height: 20px;" type="text"/>	

3.2 Use of Surveillance:

Please specify:

- YES
- NO

3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

Please specify:

It should be noted that the personal information collected may be used for statistics and trend analysis; however, as the information is stored and analysed within the PeopleSoft program, it is outside the scope of the ATS PIA.

- 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: Personal Information Transmission

Level of risk to privacy

- The personal information is used within a closed system. 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. 3
- The personal information is transmitted using wireless technologies. 4

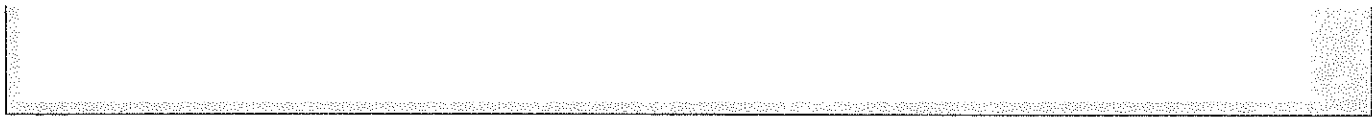
Details:

Personal information is collected on an external web server via the ATS system. On a daily basis (business days only) the information is exported in XML format to be transferred onto a second server in a secure network environment. The XML file will be downloaded to the secure server for automatic upload to PeopleSoft. The access to this location/server is limited only to the administrators of the application. The XML file will be immediately deleted from the external web server however a backup will be stored for 90 days on the secure network before being permanently deleted from the server. PeopleSoft will be the final system of records for all applicant data.

H: Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee

Details:

ATS collects Application for Employment (PIB Bank No. PSU-911) and contact information from Internet based end-users as potential candidates for internal positions. In a worst case scenario,



I: Potential risk that in the event of a privacy breach, there will be an impact on the institution

Details:

ATS collects Application for Employment (PIB Bank No. PSU-911) and contact information from Internet based end-users as potential candidates for internal positions. Exposure of applicants' personal information would

SECTION II - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Bank	Categories of Personal Information	Personal information sub-element	Type of Format	Purpose / necessity of the personal information (this column is optional)
Application for Employment Bank No. PSU-911	Name	First name* Middle name Last Name*	Electronic	To maintain an inventory of potential candidates that may be used for consideration in a staffing process when vacancies arise within the institution.
	Contact information	E-mail Address* Address (Street Number and Street Name)* City* Postal Code* Province* Country* Phone Numbers*		
	Citizenship status	Canadian Citizenship Status* Other Citizenship(s)*		
	Biographical information	Curriculum vitae* Education* Professional Certifications Designations		
	Employee personnel information	Level of security clearance*		
	Language	First Official Language Language of correspondence Language Proficiency		
	Employment Equity information	Visible Minority Information about aboriginal people Persons with disability Gender		

	Educational information	Area of study(s) Study Awards (e.g. degree)		
--	-------------------------	--	--	--

*Denotes mandatory information

Personal Information elements and sub-elements

Note: Identification of sub-elements is necessary where sensitive personal information is being collected or where the type of program or activity presents a potential privacy risk at level 2-3-4 in “Section II - Risk Identification and Categorization” of the core PIA.

Note: **Category of personal information:** This column is optional, it has been added to identify the category of personal information that will include the elements and sub-elements collected. TBS has developed a list of categories of personal information to simplify the process of describing personal information in Personal Information Banks (PIBs). It provides examples of categories and elements that can be used to summarize the personal information collected by most federal institutions. The list can be found at <http://www.infosource.gc.ca/emp/emp03.eng.asp#indexPIB>. The categories are also listed in TBS’s PIB Checklist Tool. Identifying the categories of personal information in the core PIA will make it easier to create or revise the PIB.

Personal information element: Identify each element of personal information collected (for example: 1) name, 2) home address).

Personal information sub-element: Identify sub-elements associated with each element of personal information collected (for example: 1) first name / middle initial / last name, 2) street name / street number / city / province /postal code).

Type of format: identify how the personal information will be recorded: on paper, electronically, audio recordings, visual image recordings, human biological samples or other (specify).

Purpose / necessity of the personal information: **This column is optional.** Indicate the intended purpose of collecting these elements or sub-elements of personal information and how these are demonstrably necessary for the program or activity. (“Necessary” is a higher standard than merely being useful.)

SECTION III - FLOW OF PERSONAL INFORMATION

1	Personal information is submitted into an ATS form by the applicant.
2	When the applicant 'submits' their application, their personal information gets stored in on a DMZ Server.
3	The personal information (an exported XML file generated from the database) is downloaded from the DMZ server After successful transfer to network, the personal information is deleted (purged) from the DMZ Server
4	The personal information is transferred to an HRCS Point of Contact via The XML files containing personal data are used for daily uploading to PeopleSoft. The XML files are stored on secure server location with restricted access for 3 months. After 3 months the files are permanently deleted from the network server.
5	The personal information is uploaded from the Application Server. (Out of scope for ATS) Server into the PeopleSoft

Federal government Institution responsible for program or activity:		
Identify Groups or Areas / or Divisions	Where appropriate - positions who have access or use the personal information	Geographical Location
CSE / HRCS	HRCS Point of Contact for ATS	Ottawa – Ogilvie Road
CSE / CIO	Web Team personnel	Ottawa – Ogilvie Road
Other federal government Institution responsible for program or activity:		
Non Federal Institution or Private Sector: 'name':		
Plenary		Ottawa – Ogilvie Road

SECTION IV - PRIVACY COMPLIANCE ANALYSIS

LEGAL AUTHORITY FOR COLLECTION OF PERSONAL INFORMATION

1. Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of *Privacy Act* (Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

[Additional reference here... FAA?]

YES

Please specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Personal information in support of the organization's recruitment efforts is collected in accordance with the Privacy Act under the authority of the *Financial Authority Act* Section 11.2 - Administration of HR Related Duties².

At CSE, the DGHR has been delegated the responsibility for hiring at CSE and as such, holds the authority to collect this personal information.

AND, ensure that the legal authority to collect the personal information is cited in the relevant PIB and in "Section I – Overview and PIA Initiation" of the core PIA.

Continue to Question 2

NO

If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your institution's legal advisors to determine if there is authority to proceed with the program or activity.

NECESSITY TO COLLECT PERSONAL INFORMATION

2. Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

² On the recommendation of the PSC, the Governor-in-Council approved an Exclusion of all positions and employees of the CSE (Exclusion Approval Order or EAO) from the PSEA. Essentially, the EAO removed CSE from the application of the PSEA, requiring CSE to establish its own staffing and recruitment regime. This enabled CSE to balance its sensitive security requirements, while at the same time, uphold key values of the PSEA such as merit and fairness. This EAO remains in effect today.

YES

- Ensure that all personal information necessary to administer the program or activity is listed in the relevant PIB.
- AND, implement controls and procedures to ensure the institution does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

A note is included in the Privacy Notice Statement reminding applicants to ensure information provided is **free of third party personal information and references to social insurance numbers**. The ATS application form is also designed with fields specifically requesting the type of personal information required directly from the individual. Many of those fields contain drop down lists further limiting the information that can be submitted.

Continue to Question 3

NO

- Review the proposed elements and sub-elements of personal information outlined in "Section III – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

AUTHORITY FOR THE COLLECTION, USE OR DISCLOSURE OF THE SOCIAL INSURANCE NUMBER

3. Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number*

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):

State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

Establish explicit authority through legislative amendment(s).

Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the institution is to occur on a routine or systematic basis

to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.

to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.

AND, ensure that the relevant PIB for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

Continue to Question 4

NO

- The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

Continue to Question 4.

DIRECT COLLECTION – NOTIFICATION AND CONSENT, AS APPROPRIATE

4. Is personal information collected directly from the individual to whom it relates?

Statutory reference: Sections 4 and 5 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of *Directive on Social Insurance Number*

YES

- A “**Privacy Notice**” (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must notify the individual of any of the following elements that apply (please check all appropriate boxes):
- a) The purpose and authority for the collection
 - b) Any uses or disclosures that are consistent with the original purpose.
 - c) Any uses or disclosures that are not related to the original purpose
 - d) Any legal or administrative consequences for refusing to provide the personal information
 - e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.
 - f) A reference to the PIB for the program or activity
 - g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a “**Consent Statement**” to the “**Privacy Notice**” as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose that is not listed under section 8(2) of the *Privacy Act* or a consistent use, or, to authorize indirect collection of personal information.

- The “**Consent Statement**” must include, as applicable, the following elements (please check all appropriate boxes):
- a) The purpose of the consent and the specific personal information involved.
 - b) In the case of indirect collections, the sources that will be asked to provide the information.
 - c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
 - d) Any consequences that may result from withholding consent.
 - e) Any alternatives to providing consent

- AND, implement controls and procedures to ensure that the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

Continue to Question 5

NO

- The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the institution, or from

another institution, government or third party.

Continue to Question 5

INDIRECT COLLECTION - CONSENT OR AUTHORITY PURSUANT TO SECTION 10 OF PRIVACY REGULATIONS

5. Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the *Privacy Regulations*?

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

YES

The notice and consent requirements stated at Question 4 apply. Please review the required elements listed under "YES" at Question 4 and check the corresponding boxes below to indicate the elements that need to be included in the "Privacy Notice" or the "Consent Statement" (check all that apply):

PRIVACY NOTICE	a) <input type="checkbox"/>	b) <input type="checkbox"/>	c) <input type="checkbox"/>	d) <input type="checkbox"/>	e) <input type="checkbox"/>	f) <input type="checkbox"/>	g) <input type="checkbox"/>
CONSENT STATEMENT	a) <input type="checkbox"/>	b) <input type="checkbox"/>	c) <input type="checkbox"/>	d) <input type="checkbox"/>	e) <input type="checkbox"/>		

AND, implement controls and procedures to ensure the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

Continue to Question 6

NO

Continue to Question 6

INDIRECT COLLECTION - WITHOUT NOTIFICATION AND CONSENT

6. Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices*, section 6.2.15 of the

Policy on Privacy Protection and sections 6.3.2 and 6.3.3 of *Directive on Privacy Impact Assessment*

YES

Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

a) The collection is a result of a disclosure to the institution under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

[Empty text box for explanation of subsection 8(2) disclosure]

b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided:

[Empty text box for explanation of direct notification]

c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates.

AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant PIB.

AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a core PIA for the program or activity has been adequately documented in the description of the program or activity in "Section I - Overview and PIA Initiation" of the core PIA.

OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "Privacy Notice" or the "Consent Statement" includes all of the required elements listed under "YES" at Question 4.

Continue to Question 7

NO

All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above).

All information is collected directly from the individual to whom it relates.

Continue to Question 7

RETENTION AND DISPOSAL OF PERSONAL INFORMATION

7. Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule:

ATS collects Application for Employment information retained in the Personal Information Bank PSU-911. Personal information collected within ATS will be exported on a daily basis (business days only) in XML format. Database records will be fully purged from ATS after the XML file is successfully generated. The XML file is transferred to secure network environment for automatic upload to PeopleSoft. The XML files will continue to be stored on the secure network environment for 90 days and then will be permanently deleted from the server.

The information will be retained in PeopleSoft under the following Records Disposition Authority:

CSE Retention and Disposition Schedule - 4 June 2015
21725396

The use, retention and disposition processes of this applicant information within PeopleSoft are outside the scope of the ATS PIA.

AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.

The use, retention and disposition processes of this applicant information within PeopleSoft are outside the scope of the ATS PIA.

AND, if the institution intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.

The use, retention and disposition processes of this applicant information within PeopleSoft are outside the scope of the ATS PIA.

AND, the institution must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

The standard PIB does not specifically state the RDA number, the retention period or the disposition standards for the personal information. However, it does advise the reader to contact CSE's ATIP team for those details.

Continue to Question 8

NO

- Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.
- AND, obtain a RDA from Library and Archives Canada to allow the institution, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.
- AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

NOT APPLICABLE: ATS personal information does not have a requirement to be archived at LAC.

Continue to Question 8

ACCURACY OF PERSONAL INFORMATION

8. Will all reasonable measures be adopted to ensure that personal information used by the institution for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

- Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:
 - Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.
 - A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the institution) where this is authorized, or where consent was obtained. Please briefly describe the data-matching process and the source(s) that will be used to ensure accuracy of the information:

- In cases where direct collection or consent is not feasible, the institution will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use. Please identify the sources and procedures to be used to check the accuracy of the information:

- Technological methods will be used to identify errors and discrepancies. Please briefly describe these technological methods:

- Other – please specify:

Applicant will have an option to contact CSE Human Resources by email with requests to update or correct their personal information. Upon receipt of a request, CSE Human Resources will ask the follow questions to validate:

- Confirm the job applied for
- Verify address
- Verify email and phone number
- Verify full name

Once the information is verified then the change will be made in the PeopleSoft system.

Alternatively, the applicant could also submit a formal request under the *Privacy Act* via CSE's ATIP team.

- AND, if measures are adopted other than "*direct collection or validation with the individual or with a person authorized to act on behalf of the individual*", the institution must implement appropriate controls and procedures to ensure that:
- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
 - b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
 - c) personal information can only be modified or corrected by those within the institution who have the authority to do so; and
 - d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the institution are corrected / annotated.

- AND, if appropriate, ensure that the "**Privacy Notice**" or "**Consent Statement**" and the relevant PIB are amended to identify the data-matching activity including the source(s).

Continue to Question 9

NO

- Please explain why such measures will not be adopted:

Continue to next Question 9

USE OF PERSONAL INFORMATION

9. Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the *Privacy Act*?

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of

Policy on Privacy Protection and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

YES

- Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties.
- AND, ensure that the "Data Flow Diagram" completed for "Section III – Flow of Personal Information" of the core PIA identify the areas, groups and individuals (e.g., the positions) within the institution who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.
- AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the institution will adhere to the requirements and principles in its "*Privacy Protocol For Non-Administrative Purposes*", in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

The non-administrative uses of the applicant information are within the PeopleSoft program and are outside the scope of the ATS PIA.

Continue to Question 10

NO

- Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the institution pursuant to subsection 8(2) of the *Privacy Act*:

- AND, ensure that these other uses are reflected in the relevant PIB.
- And, include a description of these other uses in the "Privacy Notice" or "Consent Statement", as appropriate,
- AND, ensure the all the other applicable requirements listed under "YES" at Question 9 are met.

Continue to Question 10

DISCLOSURES DIRECTLY RELATED TO THE ADMINISTRATION OF THE PROGRAM OR ACTIVITY

10. Will personal information be disclosed for purposes directly related to the administration of the program or activity?

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix "C" of *Directive on Privacy Impact Assessment*)

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the institution

or with other federal government institutions, please identify the branch and the program or activity.

- Within the institution for another program or activity – specify

The personal information will be disclosed to those associated with the recruitment and staffing process.

Those candidates who are successful in the evaluation process would be asked for their written consent to share personal information (name and contact information only) with Personal Security for the purpose of initiating the clearance process.

- With programs or activities of other federal government institutions – specify

Subject to applicant's consent, CSE will share information with other government department for employment purposes.³

If necessary, written consent will be obtained to provide the Public Service Commission with the applicant's name, date of birth and PRI (if applicable) for the purpose of language evaluation⁴

- Provincial, territorial or municipal governments institutions – specify

- Foreign government institutions and entities thereof – specify

- International organizations – specify

- The private sector (e.g., contractor or other external service provider) – specify

- Other – specify

- AND, ensure that:

- a) any such disclosure is made in compliance with the program or activity enabling legislation or section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;

³ This process is outside the scope of the ATS project and is not covered by the ATS PIA.

⁴ This process is outside the scope of the ATS project and is not covered by the ATS PIA.

- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the “Consistent Use” section in the relevant PIB in *Info Source*, including the specific purpose of the disclosure;
- f) the “Privacy Notice” or “Consent Statement” describes any disclosures of information; and,
- g) the “Data Flow Diagram” or “Data Flow Tables” completed in “Section IV – Flow of Personal Information” of the core PIA include details on the disclosed personal information:

The process of disclosing applicant data to other Government department is established within the PeopleSoft program and is outside the scope of the ATS PIA.

- AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:
 - o Control over personal information, where appropriate.
 - o Limitations on the collection, retention, use and disclosure of personal information.
 - o Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
 - o Measures governing the disposition of the personal information, where relevant
 - o Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
 - o Obligations are to be extended to other parties such as subcontractors.

The process of disclosing applicant data to other Government department is established within the PeopleSoft program and is outside the scope of the ATS PIA.

Continue to Question 11

NO

- There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

Continue to Question 11

ACCOUNTING FOR NEW USES OR DISCLOSURES NOT REPORTED IN INFO SOURCE

11. Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in *Info Source*?

Statutory reference: Sections 7 to 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.9 and 6.2.2 of *Directive on Privacy Practices*

YES

- Appropriate controls and procedures have been or will be implemented to ensure that:
 - a) the head of the institution or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *Info Source*;
 - b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified forthwith regarding the new consistent use;
 - c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *Info Source* will only be made with the consent of the individual to whom the information relates;
 - d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure;
 - e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate registered PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;
 - f) the Privacy Commissioner is notified forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant PIB published in *Info Source*;
 - g) the relevant PIB is amended in time for the next edition of *Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and
 - h) the Privacy Commissioner is notified prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
 - i) Other, specify

[Redacted text box]

Continue to Question 12

NO

- Please explain why such controls and procedures will not be implemented (provide adequate justification):

[Redacted text box]

Continue to Question 12

SAFEGUARDS - STATEMENT OF SENSITIVITY

12. Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment*, sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of*

Information Technology Security (MITS) and Operational Security Standard on Physical Security

YES

- The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section II - Risk Area Identification and Categorization" of the core PIA.

Continue to Question 13

NO

- Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

Continue to Question 13

SAFEGUARDS – THREAT AND RISK ASSESSMENT

13. Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity?

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment*, sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS) and Operational Security Standard on Physical Security*

YES

- Reference the title of the TRA or other security assessment in "Section VII – Supplementary Documents List:

ATS Threat and Risk Assessment 2015.doc 17489533

- AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.

- AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*.

Continue to Question 14

NO

-

Continue to Question 14

SAFEGUARDS – ADMINISTRATIVE, PHYSICAL AND TECHNICAL

14. Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Statutory reference: Sections 7 and 8 of *Privacy Act*

Policy reference: Appendix C of *Directive on Privacy Impact Assessment*, sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)* and *Operational Security Standard on Physical Security*

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

Administrative safeguards

- Internal security and privacy policies and procedures
- Staff training on privacy and the protection of personal information
- Screening and security checks of employees
- Appropriate security levels for employees who will have access to personal information
- Contingency plans and documented procedures in place to identify and respond to security and privacy breaches
- Regular monitoring of users' security practices
- Methods to ensure that only authorized personnel who need to know have access to personal information
- Other – please describe

The personal information will ultimately reside in PeopleSoft – access to PeopleSoft is restricted.

Physical safeguards**Technical safeguards**

Currently the files are transferred
procedures

There are strict security

cannot be removed from CSE premises and/or used
on non-CSE systems, unless authorization is granted by the ISSO.

In addition logs are generated to view user's access to external website.

Continue to Question 15

TECHNOLOGY AND PRIVACY - TRACKING TECHNOLOGIES

15. Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

Statutory reference: Sections 4 to 10 of the *Privacy Act and section 4 of Privacy Regulations*

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of *Directive on Privacy Practices*

YES

- The specific tracking technologies to be used is adequately described under Part F: Technology and Privacy of "Section II – Risk Area Identification and Categorization" of the core PIA;
- AND, the collection of any personal information using such technologies is reflected in the relevant PIB and in "Section III – Analysis of Personal Information Elements" of the core PIA;
- AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice";
- AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- AND, where personal information collected through such tracking technologies is used to make a

decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the Privacy Regulations.

Continue to Question 16

NO

- Tracking technologies are not used to collect personal information about users.

Continue to Question 16

TECHNOLOGY AND PRIVACY – SURVEILLANCE OR MONITORING

16. Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

Statutory reference: Sections 4 to 10 of Privacy Act, section 4 of Privacy Regulations and section 8 of the Charter of Rights and Freedoms

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of Directive on Privacy Practices

YES

- Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the Charter of Rights and Freedoms, the Privacy Act or other applicable acts.
- And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part F: Technology and Privacy of “Section II – Risk Area Identification and Categorization” of the core PIA.
- AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant PIB and in Section III – Analysis of Personal Information Elements” of the core PIA.
- AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the “**Privacy Notice**”, unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.
- If notice about surveillance or monitoring will not be provided, please explain why:
-
- AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

Continue to Question 17

NO

- The new or modified program or activity will not result in surveillance or monitoring.

Continue to Question 17

PRIVACY CONSIDERATIONS RELATED TO COMPLIANCE / REGULATORY INVESTIGATION AND ENFORCEMENT

17. Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

[Empty rectangular box for legislative authority and purpose]

AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "Section V – Privacy Compliance Analysis" and in "Section I – Overview and PIA Initiation" of the core PIA.

AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant PIB and in "Section III – Analysis of Personal Information Elements" of the core PIA.

AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

If notice about the compliance/regulatory investigation or law enforcement activities will not be provided, please explain why:

[Empty rectangular box for explanation of no notice]

NO

The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION V - Summary of Analysis and Recommendations (as applicable)

This document is a Core Privacy Impact Assessment (PIA) report for the Applicant Tracking System (ATS) and is undertaken to verify that privacy is considered with the deployment of the system. Systems that collect, process, and store information that is 'personal' in nature incur 'privacy risk' and require that security controls are implemented to ensure personal data is protected.

The ATS application **does** collect and transmit personal data, but it only stores personal information temporarily – personal data is ultimately stored in PeopleSoft. Nonetheless, ATS will be a custodian of the personal data and as such, will have to ensure the data is safeguarded to prevent disclosure, modification, and destruction. The processing and use of personal information in ATS is outside of the scope for ATS.

No ATS developer or support personnel have a need-to-know for the personal data the system processes. The following recommendations are made to ensure appropriate technical and procedural access controls are implemented in ATS to limit risk associated with processing, transmitting, and storing personal information.

Delineated Control Point:

- Data security is the responsibility of CIO while it resides in ATS and
- Assign a HRCS Point of Contact to accept data which could also be an HRCS defined automated process. HRCS assume security responsibility of data once it transferred to their Point of Contact or automated process.

Data Processing:

- Secure personal information processed in web application pages by automating the data storage process.

Data Storage:

- Implement database Identification and Authorization challenges when ATS database is being stored or retrieved.
- Implement database access control lists (ACL's) to enforce appropriate accesses.
- Identification and Authorization challenge and encryption for data

Data Transmission:

- Implement network access control lists (ACL's) to ensure data flow is restricted between authorized hosts.
- Communication path encryption for data in motion.

Other Recommendations

Consent

- Ensure that written consent is received prior to disclosing any personal information collected from the ATS to be used for any purpose not related to the original purpose, including Language testing and Security screening.
- Key elements are missing from the consent statement for disclosure of personal information to other federal department for recruitment purposes. A new statement should be drafted to clarify that consent is being requested, how to withdraw consent, and the consequences for withdrawing or not providing consent.

Disclosure

- Although outside the scope of the ATS system, formal agreements or arrangement should be implemented with any other federal department with whom CSE shares applicant data.

SECTION VI - SUPPLEMENTARY DOCUMENTS LIST

Additional documents used or related to the core PIA may include:

- Threat Risk Assessment (#17499533)
- Statement of Sensitivity (#17398701)
- Statement of Applicability (SOApp) and Security Requirements Traceability Matrix (SRTM) (#17490627)
- SA&A Client Questionnaire (#17398057)
- CSE Retention and Disposition Schedule (520-30) (#21018873)
- Security Assessment & Authorization for ATO of the Applicant Tracking System (ATS) (#23509518)

SECTION VIII – FORMAL APPROVAL

I commit to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements as they relate to the administration of this program/ activity.

I approve of this Core PIA and certify that the information contained in the document is complete and accurate.

Director, Human Resources Client Services (*print name*)

[Empty signature box]

*

Signature /Date

Director, CSE Information Management (CIO-
(*print name*))

[Empty signature box]

*

Signature /Date

Note: Responsibility for compliance with the requirements of sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage programs and activities are responsible for ensuring that privacy requirements are implemented as part of the administration of the program or activity.


As Delegated Authorities responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*, we approve this Core PIA and, based on the information provided, am satisfied that it complies with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements as they relate to the administration of this program/activity.

Director, Disclosure, Policy and Review
(*print name*)

[Empty signature box]

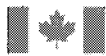
Deputy Chief, Policy and Communications
(*print name*)

Dominic Rochon

*


Signature / Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks, which must be complemented by a Core PIA, and submitted to the Treasury Board of Canada Secretariat.



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



CSE Retention and Disposition Schedule Amendment

CSE retention schedule amendment number: 3

Regarding series: 520-30 HR Applicant Eligible (disestablished)

520-40 HR Applicant Non-Eligible (disestablished)

520-30 HR Applicant (established)

Office of Primary Interest (OPI): Staffing Programs

29 April 2015

In accordance with Records Disposition Authority 97/003, issued by Library and Archives Canada, the Communications Security Establishment (CSE) has the authority to establish retention periods for records generated under the personnel security function. Establishing a retention period for these records is the joint responsibility of CSE Information Holdings Services and the OPI.

This agreement between Information Holdings Services and Staffing Programs is to disestablish series 520-30 HR Applicant Eligible and series 520-30 HR Applicant Non-Eligible, and to replace them with 520-30, HR Applicant. Files from series 520-30 HR Applicant will have the following retention: retain for 5 years after expiry of eligibility list, or five years after last administrative action, whichever is later.

The justification for this amendment is as follows: A longer retention period is required to provide a consistent retention period for applicant files across CSE.

This amendment will come into effect immediately, and will be applied to existing and future records from this series.

I, the undersigned, agree to the above changes to the retention of security applicant records:

Date

4 June 2015

Manager Staffing Administration

Date

28 May 2015



Communications Security
Establishment

Centre de la sécurité
des télécommunications



SECRET

Communications Security Establishment



Security Information Management System Applicant Tracking System THREAT AND RISK ASSESSMENT

CERRID #17489533

Revision History

<i>Version</i>	<i>Author</i>	<i>Reason for Change</i>	<i>Pages Affected</i>	<i>Date</i>
1.0		Initial document	All	Feb 2015



Executive Summary

CSE's job listing and recruitment process is currently provided by

Due to a nature of CSE's business, a new system is required such that the agency has full control over data of people applying for positions at CSE to protect their identity

The new Application Tracking System (ATS) is to be implemented before end of the fiscal year (March 31, 2015). The web component of the Applicant Tracking System (ATS) will be hosted on the existing CSE external web server (DMZ server), offering the new Internet accessible interface to job applicants. The DMZ server is a environment meaning CSE HR staffing advisors will be able to manage their published web content.

Target Residual Risk

The target risk level for this TRA is Specifically, it is below a Risk Level as calculated per the Harmonized TRA Methodology. The Recommendations Phase will propose additional safeguards to achieve this target as follows:

- Where residual risks are assessed as Low to Medium (between Risk Level 15 and 32), recommendations will be included at the discretion of the analyst and technical authority as deemed necessary;
- Where residual risks are assessed as High (above Risk Level 32), High and Very High, recommendations shall be included.

A residual risk level is appropriate for this system as the system operates in this range based on a

Assets

Information assets processed, stored, and transmitted within ATS is categorized under PIB Bank No. PSU-911 which contains "Application for Employment" information. Although ATS is not the data owner, it is a temporary data custodian and as such, must ensure data privacy security. The ATS application processes information at the Protected B level.

Other assets of the ATS application include the used to transfer applicant data from

Threats

In summary,

Accidental threats are just that – accidental, but they could lead to information compromise, modification, or deletion.

the safeguards used to address the more serious concerns will also address these accidental threats.

Safeguards and Vulnerabilities

All relevant security controls from ITSG-33 were examined in the above sections and findings are summarized here. Of the 18 ITSG-33 security control families vulnerability line items (designated V-1 through V-18), All safeguards implemented to address the other ITSG security control requirements are adequate and effective, and have a vulnerability level assessed.

Recommendations

Recommendation 1 - Perform Applicant Data Validation: The data input by external users should be validated and scanned to ensure and where possible, ATS should restrict data entry on the web form. Data validation would also improve the integrity and quality of an applicant's submission.

By implementing this recommendation, ATS

so probability of compromise must be considered leading to a overall vulnerability level for the Input Restriction and Validation control items.

Recommendation 2 – Verify Open Source Download Integrity: To limit the potential for CSE should verify the integrity of the open source software being installed on its servers. In practice, ATS is a client of the

By implementing this recommendation, ATS

As noted above (Recommendation 1), system's will so probability of compromise must be considered leading to a overall vulnerability level for the Software Integrity control item.

Document Identification

Title: Applicant Tracking System Threat and Risk Assessment

CERRID file number: #17489533

Creator:

Description: Harmonized TRA of the ATS information system.

Publisher: Communications Security Establishment (CSE)

Contributor:

Originating date: Jan 22, 2015

Last change date: Feb 24, 2015

Type: Text

Format: Microsoft Word 2010

Language: English

Rights: *Intellectual property rights – owned by Canada*
© Copyright – Her Majesty the Queen in Right of Canada - 2015



Table of Contents

Executive Summary	iii
1 Introduction and Background.....	9
1.1 Applicant Tracking System	9
1.2 Risk Management Requirements	9
1.3 Harmonized Threat and Risk Assessment Methodology.....	9
1.4 Target Residual Risk.....	9
1.5 Aim of the TRA.....	10
1.6 Scope.....	10
1.7 Limitations and Assumptions.....	11
1.8 Team Composition.....	11
2 Asset Identification and Valuation	12
2.1 General	12
2.2 System Architecture.....	12
2.3 Information	13
2.4 ATS Code	13
2.5 Personnel.....	13
2.6 Processes	14
2.7 CSE Credibility and Reputation	14
2.8 Asset Valuation	15
3 Threat Assessment	16
3.1 Threat Classes and Metrics	16
3.2 Sources of Threat Data.....	16
3.3 Threats to PB Systems	16
3.4 Summary.....	18
4 Vulnerability Assessment Phase.....	20
4.1 General	20
4.2 ITSG-33	20
4.3 Security Policy and Procedures.....	21
4.4 Access Control (AC) Family.....	21
4.5 Awareness and Training (AT) Family	22
4.6 Audit and Accountability (AU) Family	23
4.7 Security Assessment and Authorization (CA) Family	23
4.8 Configuration Management (CM) Family.....	23
4.9 Contingency Planning (CP) Family.....	24
4.10 Identification and Authentication (IA) Family	24
4.11 Incident Response (IR) Family	25
4.12 Maintenance (MA) Family	26
4.13 Media Protection (MP) Family	26
4.14 Physical and Environmental (PE) Family.....	26
4.15 Planning (PL) Family.....	26
4.16 Personnel Security (PS) Family.....	27
4.17 Risk Assessment (RA) Family	27
4.18 System and Services Acquisition (SA) Family.....	28
4.19 System and Communications Protection (SC) Family.....	28
4.20 System and Information Integrity (SI) Family	29
4.21 Summary Vulnerability Assessment.....	30
5 Calculation of Residual Risk	33
5.1 General	33



6 Recommendations 34

6.1 Recommendation 1 – Perform Applicant Data Validation 34

6.2 Recommendation 2 – Verify Open Source Download Integrity 34

Annex A - Detailed Residual Risk Table 35

Annex B - Security Control to Threat mapping..... 37

Tables

Table 1 – TRA Team Composition 11

Table 2 – Asset Valuation 15

Table 3 – Threat Assessment Table 17

Table 4 – Vulnerability Summary 31

Table 5 – High Residual Risk Items 33

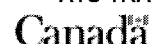
Table 6 – Recommendation 1 Risk Reduction..... 34

Table 7 – Recommendation 1 Risk Reduction..... 34

Figures

Figure 1 - ATS Architecture..... 12

Figure 2 - Threat Priority Ranking 18



1 Introduction and Background

1.1 Applicant Tracking System

CSE's job listing and recruitment process is currently provided by

Due to a nature of CSE's business, a new system is required such that the agency has full control over data of people applying for positions at CSE to protect their identity

The new Application Tracking System (ATS) is to be implemented before end of the fiscal year (March 31, 2015). The web component of the Applicant Tracking System (ATS) will be hosted on the existing CSE external web server (DMZ server), offering the new Internet accessible interface to job applicants. The DMZ server is a environment meaning CSE HR staffing advisors will be able to manage their published web content.

1.2 Risk Management Requirements

The Policy on Government Security (PGS) requires deputy heads to establish a security program for the coordination and management of departmental security activities. This basic policy requirement is amplified in the Directive on Departmental Security Management (DDSM (TBS document)) which calls for appropriate security measures when accessing, storing, transmitting and disposing of information.

With respect to IT systems such as ATS, the effectiveness of these safeguards must be assessed before the system is authorized to commence operation, and monitored continuously thereafter to identify new threats or vulnerabilities, and to address any deficiencies. With this in mind, the Operational Security Standard: Management of Information Technology Security (MITS, a TBS document) prescribes the Threat and Risk Assessment (TRA) a mandatory analytical tool to identify unacceptable risks for corrective action.

Security Assessment and Authorization (SA&A) are complementary processes for verifying and validating IT security controls and authorizing IT systems to commence operation. SA&A was formally known as Certification and Accreditation (C&A). ATS requires a formal SA&A process.

1.3 Harmonized Threat and Risk Assessment Methodology

This TRA has been prepared in accordance with the Harmonized Threat and Risk Assessment (HTRA) Methodology issued jointly by Communications Security Establishment Canada (CSEC) and the Royal Canadian Mounted Police (RCMP). The analysis is performed in five distinct phases as follows:

- Statement of Sensitivity;
- Threat Assessment;
- Vulnerability Assessment;
- Calculation of Residual Risk; and
- Recommendations.

1.4 Target Residual Risk

The target risk level for this TRA is Specifically, it is below a Risk Level as calculated per the Harmonized TRA Methodology. The Recommendations Phase will propose additional safeguards to achieve this target as follows:

- Where residual risks are assessed as Low to Medium (between Risk Level 15 and 32), recommendations will be included at the discretion of the analyst and technical authority as deemed necessary;
- Where residual risks are assessed as High (above Risk Level 32), High and Very High, recommendations shall be included.

A residual risk level is appropriate for this system as the system operates in this range based on a

1.5 Aim of the TRA

The aim of this TRA is to verify that the ATS system protects itself and other relevant assets of CSE including the personal information of staff, contractors, internees, clients and partners.

The TRA is used to assess the need for security controls beyond current baseline security controls, identify the key risk areas that could potentially lead to a security exposure or compromise of sensitive information or other assets, and propose mitigation strategies to reduce residual risk to meet the target residual risk. This assessment focuses on the adequacy and effectiveness of safeguards to ensure vulnerability levels are very low.

1.6 Scope

The system Concept of Operations (ConOps) can be viewed at [ATS SA&A ConOp \(#14425708\)](#). This document and the companion [ATS ConOp OV&SV Diagrams \(14424814\)](#) document illustrate the boundaries of the system, and describe the approach to system and security management.

1.6.1 In Scope

The following elements of ATS are in scope for analysis for this TRA.

- Information:
 - Applicant Data
- Software
 - ATS Code
- Support Personnel
 - CIO Web Team

1.6.2 Out of Scope:

Specific elements out of scope are:

- The existing web server
- Other non-system-specific servers and networks;
- Common hardware, software, and security service assets;
- CSE workstations;
- Non system-associated personnel, security programs, processes and procedures;
- The physical facility's environmental security capabilities; and
- Personnel security capabilities.

The existing web server has already been assessed and has authority to operate. Refer to CERRID folder #1000239 for SA&A documents.

1.7 Limitations and Assumptions

The following limitations apply to this TRA.

- Applicant Tracking System is not responsible to build, manage, or support network components, server operating systems, virtual hosting systems, workstation desktops, database instances, or web services. The adequacy and effectiveness of safeguards in these systems is assumed to be appropriate to host the Applicant Tracking System application.
- Applicant Tracking System is not responsible to build, manage, or support the existing web server. The adequacy and effectiveness of safeguards in these systems is assumed to be appropriate to host the Applicant Tracking System application.

1.8 Team Composition

The following table identifies the core team members with their primary responsibilities or inputs, and other resources available to help complete the TRA.

Table 1 – TRA Team Composition

<i>Organization</i>	<i>Team Member(s)</i>	<i>Primary Responsibilities</i>
CSE		
CSE		
CSE		
CSE		
CSE		

2 Asset Identification and Valuation

2.1 General

The purpose of the Asset Identification and Valuation (also referred to as the Statement of Sensitivity) is to list the assets that are deemed to be most sensitive or critical. The value of each asset is expressed in terms of Confidentiality, Integrity, Availability and Replacement Value (where applicable) as well as the relative assessed value. Each assessed value is determined by evaluating the impact of compromise.

The Harmonized TRA Methodology defines assets as “*tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.*”

The HTRA assigns assets to four broad classes, namely people, tangible assets, services/processes and intangible assets. People, working with tangible assets such as information systems like ATS, produce services, the quality of which affects intangible assets such as employee morale, client satisfaction, and corporate reputation. As a general rule, most security controls are applied directly to people and tangible assets even though the ultimate goal of these safeguards is to protect service delivery, maintain client satisfaction, and keep employee morale high. With this in mind, the asset identification process within a TRA typically concentrates on tangible assets and personnel inherent to the system but this TRA will include the intangible assets due to the privacy concerns associated with the applicant data.

2.2 System Architecture

Figure 1 - ATS Architecture

2.3 Information

Information assets processed, stored, and transmitted within ATS is categorized under PIB Bank No. PSU-911 which contains "Application for Employment" information. The PIB describes this information as follows.

This bank describes personal information related to individuals who have submitted applications for employment or provided curricula vitae (solicited or unsolicited) and related correspondence. The personal information provided by individuals on application forms, curricula vitae, and correspondence may include: name, contact information, employment status and history, educational background, marital status, date of birth, gender, official language proficiency, employment equity, physical disability considerations, citizenship, Personal Record Identifier, Client Server Number, transcripts, letters of recommendation, and other personal information.

The information asset, which will subsequently be known as "applicant data", is considered to be at the **Protected B** level. There is no availability value to applicant data since ATS is only a conduit to getting it to the PeopleSoft application – the PeopleSoft application has to consider availability of applicant data. Applicant data has an integrity value of since a compromise of data integrity would

2.4 ATS Code

The ATS application is

Web technologies include

ATS Code has no confidentiality value, but it does have integrity and availability values. For obvious reasons, the integrity of the ATS Code should be sustained to ensure applicant data is collected, transmitted, and stored accurately. Compromise of the integrity of applicant data could cause

2.5 Personnel

Access to Applicant Tracking System (ATS) is governed by internal CSE policy which restricts administrative access to CSE employees and contractors. Administrative and support access is restricted to only CSE employees or contractors working within the ATS environment. Admin and support users are CIO personnel.

People have no confidentiality or integrity values for the following reasons.

- Section 4.2.2 of the HTRA states "human beings are not normally assigned confidentiality values".
- Section 4.2.4 of the HTRA states "... people are not assigned integrity values in the context of the HTRA Methodology".

Section 4.2.3 of the HTRA indicates that availability values (of people) are generally derived from the importance of the services they support" which is negligible for end-users. In the long term, unavailability of the ATS support staff resources could affect the HR business process, but there are a number of qualified individuals that could support the ATS service. There would be little impact on other ATS assets

if individual staff members were unavailable for short periods of time so CIO personnel have a availability value.

End-users have no administrative or support capabilities and therefore, they have no asset value to the ATS system. CSE personnel associated with common network and network security services are considered out-of-scope.

2.6 Processes

There are three ATS processes that have value and need to be examined in the ATS Threat and Risk Assessment (TRA).

1. Exporting the applicant data from the DMZ server
2. Forwarding the applicant data to the PeopleSoft point of contact or authorized automated process.
3. Purging the applicant data from the DMZ server and

Confidentiality of the processes (e.g. disclosure of the steps involved in the processes) is not sensitive. However, they must have integrity and function as expected to prevent
If these processes are not accurately followed they could cause injury commensurate with those described in the level physiological category. Logically, if processes are unavailable it means

2.7 CSE Credibility and Reputation

2.8 Asset Valuation

The following table shows the relatively small number of ATS assets along with their associated values.

Table 2 – Asset Valuation

Class	Category	Group	Subgroup	Component or Individual	Asset Value				
					C	I	A		\$
							i	o	
Tangible	Information								
	Software ¹								
People	Personnel								
Processes									
Intangible	Internal								
	External								
Legend C – Confidentiality Value. I – Integrity Value. A – Availability Value. i – Intrinsic Availability Value for Personnel. o – Operational Availability Value for Personnel. \$ - Replacement Cost.									

3 Threat Assessment

3.1 Threat Classes and Metrics

The HTRA organizes threats into three broad classes, namely: deliberate threats, accidents, and natural hazards. In a threat assessment, the likelihood or probability of relevant threats actually occurring is assessed, followed by an evaluation of the capability of deliberate threat agents or the gravity of accidents and natural hazards to establish an overall threat rating from Very Low to Very High for each threat agent. This threat assessment is structured and presented accordingly.

3.2 Sources of Threat Data

The following threat assessment is based upon the CIO “CSE PB Threat Assessment” document (#10277208). Rationale for threat level ratings can be found in Section 3.2 of the document.

3.3 Threats to PB Systems

Table 3 – Threat Assessment Table

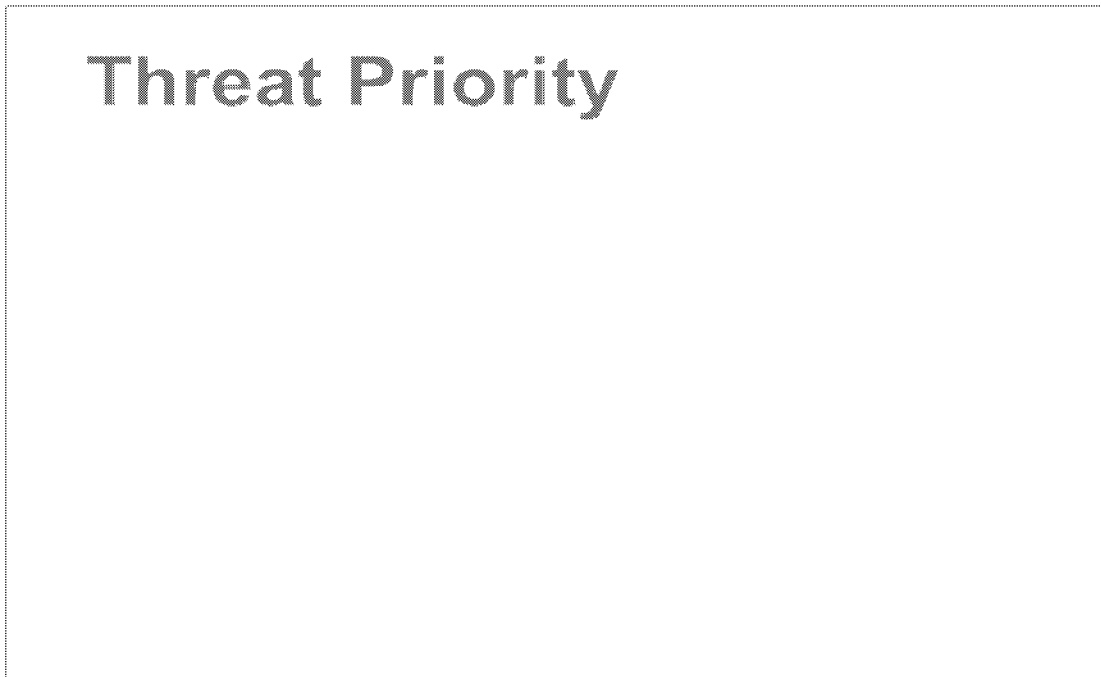
Threat Class	Threat Activity	Threat Agent	Threat Event	Likelihood	Impact	Threat Level	Threat Level Affecting			Asset Group(s) Affected
							C	I	A	
Deliberate										
Deliberate										
Accidents										
Accidents										



Threat Class	Threat Activity	Threat Agent	Threat Event	Likelihood	Impact	Threat Level	Threat Level Affecting			Asset Group(s) Affected
							C	I	A	
Natural										

Adding additional security controls to address _____ will have a cost, but the result will be an overall reduction of risk based on mitigation of key threat areas. When thinking about enhanced security controls, the TRA considered the following ranking of threat priority.

Figure 2 - Threat Priority Ranking



3.4 Summary

In summary,

Accidental threats are just that – accidental, but they could lead to

In general, all other accidental threats are at a or level. Presumably the safeguards used to address the more serious concerns will also address these accidental threats.



4 Vulnerability Assessment Phase

4.1 General

As noted in Section 4.1 of the HTRA, vulnerabilities are inversely proportional to safeguard effectiveness. In essence, more robust security measures reduce vulnerabilities, whereas less effective safeguards are more vulnerable to exploitation.

Some vulnerabilities reflect weak prevention mechanisms, and thereby increase the probability of compromise should a threat event actually occur. Others arise from weak detection, response and recovery mechanisms which increase the severity of a successful threat event.

4.2 ITSG-33

ITSG-33 was prepared by CSE pursuant to the Responsibilities of Lead Security Agencies outlined in Appendix B of the PGS, in this case for “developing guidelines and tools related to IT security”. Annex 3 to ITSG-33, the Security Control Catalogue, provides a collection of security controls and control enhancements categorized in three broad classes, namely: management, operational, and technical security controls. Each class is subdivided into families as follows:

- **Management Security Controls**
 - Planning (PL)
 - Risk Assessment (RA)
 - Security Assessment and Authorization (CA)
 - System and Services Acquisition (SA)
- **Operational Security Controls**
 - Configuration Management (CM)
 - Contingency Planning (CP)
 - Incident Response (IR)
 - Maintenance (MA)
 - Media Protection (MP)
 - Physical and Environmental Protection (PE)
 - Personnel Security (PS)
 - Awareness and Training (AT)
 - System and Information Integrity (SI)
- **Technical Security Controls**
 - Access Control (AC)
 - Audit and Accountability (AU)
 - Identification and Authentication (IA)
 - System and Communication Protection (SC)

This assessment focuses toward the Technical Security Controls identified as relevant to an application, as identified in the Statement of Applicability (SOApp) - SRTM – (PB) document. While many security controls have been implemented within ATS’s hosting environment, even more are provided by the

Nonetheless, these safeguards are out of scope since they are managed by other CSE IT teams. Non-applicable control items of the following ITSG-33 security families are not analyzed.

- The IT infrastructure provides most Audit and Accountability (AU), Incident Response (IR), and Maintenance (MA) security controls.
- Physical and Environmental Protection (PE) and Media Protection (MP) security controls are provided by CSE data centers.

- Awareness and Training (AT), Personnel Security (PS), and System and Services Acquisition (SA) security controls are implemented at the department level.

4.3 Security Policy and Procedures

The first security control in each family requires a documented security policy, with more detailed standards and procedures for implementing the policy in practice. In this regard, CSE has a number of overarching security policies that can be found on the Intranet

Those related to IT include:

- CSE Asset Management Policy
- Accountability Framework for CSE Security
- Security Incidents and Investigations
- Protecting and Classifying Information
- Electronic Information Security Policy Framework

There are also a large number of standards, procedures, directives, instructions and guidelines available at the Intranet web site. Since there is not a lack of policy and procedures for information technology (IT) and information management (IM) there is a level vulnerability to threats due to probability of compromise and severity of outcome since the safeguard is very effective.

4.4 Access Control (AC) Family

Access controls for the ATS application must be implemented to ensure Internet end-users have access to the ATS application but not to ATS administration consoles. There are three distinct account types in ATS with clearly delineated access rights that enforce Separation of Duties (AC-5) and Least Privilege (AC-6) principles: end-user, ATS Content Administrators, and Administrators. A Admin account has all privileges in the system, the ATS Content Admin only has privileges to manage the ATS web site content, and end-users can only access the ATS application, complete the ATS web form, and submit their application.

Account Management (AC-2) is handled based on the type of account:

- The Admin account is a member of CIO
- ATS Content Admin accounts are members of the HRCS business unit (Human Resources); and
- There are no end-user accounts – any person online can access ATS to apply for a position.

and ATS Content Admin accounts will be created using and unsuccessful Login Attempts (AC-7) will be captured by and stored in its

End-users do not login to ATS and as a rule; ATS does not want to impose a session lock since it could interfere with the applicant's submission so the Session Lock (AC-11) control item is not applicable to them.

ATS security controls are implemented under the assumption that applicant data is always at the Protected B level

In summary, ATS uses a combination of _____ in conjunction with equally effective identification & authentication (I&A), which is examined below. ATS also has audit capability (also examined below) that could provide active response measures to compliment the preventative AC security controls. The probability of compromise due to weak access controls is _____ and there are

_____ which results in an overall _____ vulnerability level.

4.5 Awareness and Training (AT) Family

Although AT security controls are not included in the SRTM for applications but they are a powerful security control since alert and well-informed employees are much less likely to make compromising mistakes, and much more likely to detect and respond to security anomalies.

CSEC, in general, provide a high level of security awareness briefings, communications, and classroom training (AT-3) on a continuous basis. The security culture of the department is very mature, and each employee and contractor in the ATS project is committed to comply with the various departmental security policies, directives and standards.

The Agency and the project team members have a good level of security awareness and it is very likely that they have the ability to detect and respond to IT security issues and concerns for a probability of compromise and severity of outcome. The overall vulnerability level for this security control family is

4.6 Audit and Accountability (AU) Family

The security controls and control enhancements of the Audit and Accountability (AU) family provide effective support to Incident Response (IR) security controls. ATS has application audit capability whereby all activity is captured for investigative purposes. has the capacity to define Auditable Events (AU-2), the Content of Audit Records (AU-3), and Audit Storage Capacity (AU-4) but has implemented default audit configurations.

ATS leverages the for its audit capability. For instance,

In short, current audit processes are controlled by groups outside of CIO ATS has audit enabled and as such, provides audit information to the team. For ATS, the vulnerability level for AU security controls is

4.7 Security Assessment and Authorization (CA) Family

Certification & Accreditation (C&A) are mandatory requirements of Section 12.3.3 of MITS. Certification provides a known level of assurance or confidence that the right safeguards have been implemented and installed correctly, while accreditation is a formal authorization to commence processing with a known and acceptable level of residual risk. Although the terms have changed with ITSG-33 to Security Assessment (certification) and Authorization (accreditation), or SA&A, the procedures and the objectives remain substantially the same.

ATS is undergoing a formal SA&A (CA-6) process that includes a Security Assessment (CA-2) (i.e. this report), and will create a System Security Plan to meet the Plan of Action and Milestones (CA-5) requirement. Continuous Monitoring (CA-7) of the system is a standard procedure of the for CSE systems, and formal Authorization is only given for periods of time which forces systems to be continuously re-assessed.

The CA control family does not introduce vulnerabilities so there is a probability of compromise and severity of outcome for an overall vulnerability level of

4.8 Configuration Management (CM) Family

Configuration management is essential for informed decision making and for the maintenance of system accreditation throughout the system's life cycle. ATS not has produced a detailed 'build' document that could be considered the Baseline Configuration (CM-2), but ATS software components are installed using default parameters meaning the baseline Configuration Settings (CM-6) could be reproduced.

CSE has an established Change Management Board that provides a forum for Configuration Change Control (CM-3). Change proposals include a Security Impact Analysis (CM-4). While anyone may initiate a change proposal, only the Change Management Board may approve formal requests for change.

ATS's configuration management regime is effective, leaving a _____ overall vulnerability level due to a _____ probability of compromise and severity of outcome.

4.9 Contingency Planning (CP) Family

According to Section 12.8 of MITS, IT systems that support critical services must have a Business Continuity Plan (BCP). ATS is not considered a mission critical system so it does not need to be in the Agency's BCP, but it should have some contingency planning to ensure it can be rebuilt if a catastrophic event or failure occurs.

A Contingency Plan (CP-2) for ATS is essentially

The probability of compromise (i.e. catastrophic failure) of the Production ATS server
ATS has an adequate backup and system recovery/reconstitution process the gravity of a catastrophic failure _____ an overall vulnerability level of _____

4.10 Identification and Authentication (IA) Family

In practice, Identification and Authentications (Organizational Users) (IA-2) are enforced since all development and administration components of the ATS application enforce user identification and

authentication,

The server uses a

Since there are no functions that can be performed without logging in the probability of compromise through authorized I&A channels the severity of outcome safeguards are effective. A vulnerability level of is realised for this family of security controls.

4.11 Incident Response (IR) Family

Although Incident Response (IR) at the server and network levels in and of themselves are not a function of the ATS project team, the application needs to have adequate self-monitoring and response processes in place to ensure it is not the 'weak link' in CSE's DMZ environment.

CSE has appropriate incident response policies and guidelines in place which can be found on the Intranet web site. As per SEC-405-1 Information Technology Security Incident Response Standard (CSE document), Incident Handling (IR-4) is a function of CIO. Within CIO is responsible for Incident Handling (IR-4) and Incident Monitoring (IR-5). Incident Reporting (IR-6) can be done by any CSE individual. Annex A of SEC-405-1 outlines incident categories based on where they occur (i.e. internal network, external cyber threat, and network operations), provides a description/example of the incident, and a Primary and Supporting response lead.

Since Incident Response functions are handled by other CSE teams the vulnerability level for ATS personnel is for this family of security controls.

4.12 Maintenance (MA) Family

The Maintenance family of security controls are not present in CIO- s SoApp/SRTM for applications spreadsheet, but maintenance controls contribute to the security posture of ATS. A high level assessment will be made to ensure there are no gaps that may seriously impact the security posture of ATS.

CSE enforces a Controlled Maintenance (MA-2) approach for all of its IT assets ensuring system maintenance is done in a timely manner by qualified individuals with appropriate authorization to have physical accesses to devices. With regard to controlling Maintenance Tools (MA-3), CSE have clearly defined network usage policies that stipulate the use of network maintenance tools can only be used by groups that perform maintenance and/or investigative functions. Further to this,

CSE maintenance practices provide adequate prevention and detective security controls, and the abilities for support teams to provide Timely Maintenance (MA-6) enhance the overall maintenance capability. probability of compromise (adequate prevention) and severity of outcome (adequate detection and response) indicate a vulnerability level for the Maintenance security control family.

4.13 Media Protection (MP) Family

Media Protection controls also fall outside the responsibility of ATS, are a part of the overall operation of the application. CIO personnel transfer applicant data on the DMZ server on a workstation.

Workstations on

The ability to prevent use of on workstations and to prevent data loss through the use of probability of compromise of applicant data.

since only authorized individuals would be capable of accessing files on it. probability of compromise with severity of outcome indicates a overall vulnerability level for this control.

4.14 Physical and Environmental (PE) Family

Physical and Environmental (PE) controls provide critical security functions for all IT systems, but are out of scope for the ATS TRA. Even so, there are no concerns with the physical security of the MTA facility and its data centers so a overall vulnerability level is assessed.

4.15 Planning (PL) Family

A formal System Security Plan (PL-2) is followed at CSE for all IT systems, as is Security Related Activity Planning (PL-6). Security activity calls for the following documents to be created and presented as SA&A evidence.

- SA&A Client Questionnaire
- Preliminary Privacy Impact Assessment (PPIA) (PL-5)
- Concept of Operations (ConOp) (PL-2(1))
- Statement of Sensitivity (SOS)
- Statement of Applicability (SOApp) and Security Requirements Traceability Matrix (SRTM)
- Threat and Risk Assessment (TRA)
- System Security Plan (SSP – to be created post TRA)

As part of its System Security Plan (PL-2), ATS

all public and internal facing interfaces were security assessed when this the portal service went into a production state. The ATS ConOps document (#17525650) discusses roles and privileges for ATS users, unique security requirements, and the types of information processed, stored and transmitted. ATS is not a mission critical system and would not take restoration priority over other applications and/servers of the Agency.

CSE issues department wide Rules of Behaviour (PL-4), which effectively are the acceptable use policy providing guidance for rules of behaviour. There are a number of subordinate policies, standards, directives and guidelines the set rules for information management and protection.

ATS has undergone a Privacy Impact Assessment (PL-5) (PIA) which has obviously indicated personal information will be transmitted, processed, and stored by the application. However, it must be noted that ATS merely transports applicant data to the PeopleSoft system on behalf of HRCS. ATS does not the final destination for applicant data and it does not store it for future use and therefore, is not required to create the PIB. Even so, ATS has implemented logical security controls to ensure personal data is communicated, temporarily stored, and transferred to PeopleSoft such to comply with privacy requirements.

The overall impact of ATS compliance to the PL family of security controls is appropriate and the application has addressed key items within this group. Since there are no concerns related to this control family the overall vulnerability level is

4.16 Personnel Security (PS) Family

Personnel Security (PS) control items are also out of scope for this assessment, but in practice, all CSE employees and contractors have a minimum Level III Personal Screening (PS-3) which authorizes them to work on the and networks. Support teams working in data centers all have Level III Personal Screening (PS-3) which authorizes them to have privileged accesses to servers, permitting them to perform their duties.

There are no concerns with PS security controls for this assessment so a vulnerability level is assessed.

4.17 Risk Assessment (RA) Family

The TRA is a structured analytical process to support informed security risk management. As such, this report satisfies mandatory requirements of the DDSM, Section 12.3.2 of MITS, and the Risk Assessment (RA-3) security control in ITSG-33. Furthermore, the Statement of Sensitivity reflects an objective Security Categorization (RA-2) thereby conforming to TBS security policy instruments.

Vulnerability Scanning (RA-5) is an effective technique for identifying security weaknesses that might expose IT assets to unacceptable risks. CSE perform vulnerability scans on all servers prior to their implementation into a production environment. Further to this, CIO- has requested be performed on key DMZ servers, most of which are used by ATS. The overall vulnerability to ATS for

this family is presuming a vulnerability scan will be performed on the ATS production servers prior to a Full Authority to Operate is issued.

4.18 System and Services Acquisition (SA) Family

ATS software components are all open source and as such, Information System Documentation (SA-5) is available online and Software Usage Restrictions (SA-6) are not applicable. Admin team members

With regard to Security Engineering Principles (SA-8), the

Developer Configuration Management (SA-10) has a number of requirements which are discussed here, but have related controls in the Configuration Management (CM) family – particularly CM-3, CM-4, CM-6, and CM-9 which were addressed above. Configuration management is performed using

For developer Security Testing (SA-11) The ATS developers use the security controls implemented by CIO which includes the following.

A vulnerability assessment was performed on the hosting web server, and subsequent scans are performed on a monthly basis (by CIO). All of the SA security control items are adequately addressed probability of compromise and severity of outcome for an overall vulnerability of

4.19 System and Communications Protection (SC) Family

The ATS application has different access points:
so Application Partitioning (SC-2) is achieved.

The ATS application uses _____ and for _____ protect the integrity of transmitted packets and therefore, enforce Transmission Integrity (SC-8). _____ also enforce Transmission Confidentiality since packet payloads _____ as well as Session Authenticity (SC-23) to protect against _____ terminates communication sessions after a period of inactivity to enforce Network Disconnect (SC-10).

For Use of Cryptography (SC-13), CIO

The public facing content of the ATS application can only be modified by HRSC personnel and should therefore remain appropriate. The availability of the ATS application relies

Nonetheless, Public Access Protections (SC-14) also include some security controls of the System & Information Integrity (SI) family examined below.

Therefore, the project meets the objectives of the Architecture and Provisioning for Name/Address Resolution Service (SC-22) control item.

For Session Authenticity (SC-23),

Applicant information is stored in the

data is

to be used for the transfer of applicant

The controls noted above provide effective preventative security _____ probability of compromise. The Agency's network, server, and workstation monitoring services provide a very effective detection and response environment _____ severity of outcome since compromises would be quickly detected and damage would be contained. Overall, there is a _____ vulnerability level for SC security control items.

4.20 System and Information Integrity (SI) Family

The security controls of the System and Information Integrity (SI) family generally support other security controls. For example, Flaw Remediation (SI-2), Information System Monitoring (SI-4), Security Alerts, Advisories and Directives (SI-5) and Software and Information Integrity (SI-7) are closely related to Audit and Accountability (AU), Incident Response (IR), Maintenance (MA), and Risk Assessment (RA) controls. Information Input Restrictions (SI-9) are achieved with Access Control (AC) and Identification and Authentication (IA) security controls, as well as through the Protection of Information at Rest (SC-28). Error Handling (SI-11) is also addressed with Audit and Accountability (AU) and Incident Response (IR) security controls, while Information Output Handling and Retention (SI-12) is somewhat similar to portions of Information System Backup (CP-9).

Even so, relevant security controls warrant some analysis, especially in light of the [redacted] and [redacted] threats identified earlier. Of importance,

but these safeguards are under CIO [redacted] control and as such, are out of scope for ATS servers and workstations.

[redacted] on both network workstations [redacted] each time it is used to transfer applicant data.

Information System Monitoring (SI-4) can only be achieved in ATS for [redacted] and Web Content Admin accesses and activity, so only these events are assessed here. Only the [redacted] Admin account can manage [redacted] audit configurations and audit log files; non-privileged users, such as Web Content Admins and end-users, have no logical accesses to these. CIO [redacted] responds to incidents as per SEC-405-1 - Information Technology Security Incident Response Standard. As noted in the SEC-405-1 standard, [redacted] are to coordinate with [redacted] to implement appropriate logging and monitoring capabilities for information systems.

For Software and information Integrity (SI-7), ATS code integrity is enforced using [redacted]

ATS error events are all generated by [redacted] software components and do not contain any applicant data elements. ATS has effective Error Handling (SI-11) controls in that [redacted]

[redacted] These teams are aware of their requirement to comply with the procedures outlined in the ITSM Policy (#784662) and ITSM Incident Management Standards (#876296).

ATS only facilitates the transfer of applicant data between the end-user and HR and therefore, are not responsible for handling and retaining it for its life cycle in PeopleSoft. ATS has performed a PIA and understands its responsibilities to protecting applicant data while it is under ATS control. In practice, applicant data will only be accessed by CIO [redacted] personnel through the [redacted] console to be transferred onto the [redacted] and subsequently be given to the appropriate HR point-of-contact for transfer to PeopleSoft. At no time will applicant data be read or altered by CIO [redacted] personnel, and will only be deleted on the [redacted] and in the ATS application once HRCS confirm it has been successfully transferred into their environment. (Information Output Handling and Retention (SI-12)).

4.21 Summary Vulnerability Assessment

All relevant security controls from ITSG-33 were examined in the above sections and findings are summarized here. Of the 18 ITSG-33 security control families vulnerability line items (designated V-1 through V-18),

Table 4 – Vulnerability Summary

ID	Vulnerability	Relevant Vulnerability	Level	Asset Exposed	Threats Facilitated
V-1	Security Policies & Procedures				
V-2	Access Control (AC)				
V-3	Awareness & Training (AT)				
V-4	Audit & Accountability (AU)				
V-5	Security Assessment & Authorization (CA)				
V-6	Configuration Management (CM)				
V-7	Contingency Planning (CP)				
V-8	Identification & Authentication (IA)				
V-9	Incident Response (IR)				
V-10	Maintenance (MA)				
V-11	Media Protection (MP)				

ID	Vulnerability	Relevant Vulnerability	Level	Asset Exposed	Threats Facilitated
V-12	Physical & Environmental (PE)				
V-13	Planning (PL)				
V-14	Personal Security (PS)				
V-15	Risk Assessment (RA)				
V-16	System & Services Acquisition (SA)				
V-17	System & Communications Protection (SC)				
V-18	System & Information Integrity (SI)				

5 Calculation of Residual Risk

5.1 General

To calculate residual risks in an IT system each threat agent is paired with the vulnerabilities that expose the affected assets to compromise. Then, the product of the three variables (asset value, threat, and vulnerability) is computed in accordance with the procedures outlined in Annex E of the HTRA. The resulting Residual Risk can assume values between 1 and 125 divided into levels as shown in the table below:

<i>Residual Risk Value</i>	1-4	5-12	15-32	36-75	80-125
<i>Risk Level</i>	Very Low	Low	Medium	High	Very High

The assessment will only concentrate on the more serious threats and vulnerabilities which are those in the High or Very High ranges. The full Risk Calculation table can be seen in Annex A.

6 Recommendations

All unacceptable residual risks may be reduced to a satisfactory level with the approval and implementation of the following interrelated recommendations.

6.1 Recommendation 1 – Perform Applicant Data Validation

The data input by external users should be validated and scanned and where possible, ATS should restrict data entry on the web form. Data validation would also improve the integrity and quality of an applicant's submission.

By implementing this recommendation, ATS

However, compromise must be considered leading to a overall vulnerability level for the Input Restriction and Validation control items. so probability of

6.2 Recommendation 2 – Verify Open Source Download Integrity

To limit the potential for CSE should verify the integrity of the open source software being installed on its servers. In practice, ATS is a client of the

By implementing this recommendation, ATS

As noted above (Recommendation 1), system's considered leading to a overall vulnerability level for the Software Integrity control item. so probability of compromise must be

Annex A - Detailed Residual Risk Table

Asset	A _{val}			Threat	T	ID	Vulnerability	V	R
	C	I	A						
Information									



Software
Processes
IT Staff

Annex B - Security Control to Threat mapping

Event	Mitigating Security Control (Safeguard)
--------------	--

Event	Mitigating Security Control (Safeguard)
-------	---

**Government of Canada Key Management Infrastructure
(GC KMI)**

Core Privacy Impact Assessment

(CERRID # 28818724)

Final

Version 1.0

24 May 2016

Page intentionally blank

s.15(1) - DEF

RECORD OF AMENDMENTS

Version	Date	Author(s)	Amendment(s)
0.1	23 Jan 2015		Initial draft to ATIP for review and feedback.
0.2	23 Feb 2015		Draft to for review and feedback.
0.3	27 April 2015		Draft to and for comments.
0.4	25 August 2015		Incorporated ATIP input on PIBs.
0.5	22 September 2015		Incorporate GC KMI User Registration forms. Update User registration process. Final draft to ATIP for comments.
0.6	January 2016		Incorporate ATIP and process input.
0.7	13 May 2016		Incorporate ATIP feedback / comments.
1.0	24 May 2016		Incorporate ATIP Office comments.

Page intentionally blank

Table of Contents

Record of Amendments	- 3 -
1 Overview and Privacy Impact Assessment (PIA) Initiation	- 7 -
1.1 Government Institution.....	- 7 -
1.2 Name of Program or Activity of the Government Institution	- 7 -
1.3 Description of Program or Activity.....	- 7 -
1.4 Description of the class of records associated with the program or activity ...	- 8 -
1.5 Legal Authority for Program or Activity	- 10 -
1.6 Summary of the project / initiative / change	- 10 -
2 Risk Identification & Organization.....	- 11 -
2.1 A: Type of Program or Activity	- 11 -
2.2 B: Type of Personal Information Involved and Context.....	- 12 -
2.3 C: Program or Activity Partners and Private Sector Involvement.....	- 13 -
2.4 D: Duration of the Program or Activity	- 13 -
2.5 E: Program Population.....	- 14 -
2.6 E: Technology and Privacy	- 14 -
2.7 G: Personal Information Transmission.....	- 16 -
2.8 H: Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee.....	- 16 -
2.9 I: Potential risk that in the event of a privacy breach, there will be an impact on the institution	- 17 -
3 Analysis of Personal Identification Elements for the Program or Activity.....	- 18 -
3.1 Acquisition, Storage, Handling and Modification.....	- 19 -
4 Flow of Personal Information for the Program or Activity	- 21 -
5 Privacy Compliance Analysis	- 22 -
6 Summary of the Analysis and Recommendations	- 25 -
7 Supplementary Documents List.....	- 25 -
8 Formal Approval.....	- 27 -
Appendix A – Sample GC KMI Applicant Registration Forms.....	- 29 -

Page intentionally blank

1 Overview and Privacy Impact Assessment (PIA) Initiation

1.1 Government Institution

Communications Security Establishment (CSE).

Government Official Responsible for the Privacy Impact Assessment	Head of government institution / Delegate for section 10 of the Privacy Act.
Joseph Waddington, DG CP, CSE	Dominic Rochon, DC PC, CSE

1.2 Name of Program or Activity of the Government Institution

Government of Canada Key Management Infrastructure (GC KMI).

1.3 Description of Program or Activity

This Core PIA describes how CSE will protect personal information collected and stored for the exclusive purpose of registering users for access to the GC KMI being developed at CSE. Subsequently, this PIA assesses the privacy implications of GC KMI registration and describes mitigation processes to address privacy risks.

The Government of Canada (GC) is increasingly dependent on distributed information technology, both for command and control and for normal business operations. A major concern with respect to electronic information delivery is the preservation of the confidentiality of nationally sensitive (classified) information. This is normally accomplished through encryption of information in transit and/or storage. Within the GC, cryptographic keying material, equipment and systems used to protect nationally sensitive information are categorized as High Assurance and must be approved or endorsed by CSE, the Canadian government Communications Security (COMSEC) Authority. Keying material used by GC departments is generally produced at CSE (or Allied equivalents) and distributed to the departments for use. Electronic key management is intended to reduce the exposure of encryption keys while they are in transit within the cryptographic management system, and to increase the cost-effectiveness and flexibility of cryptographic key handling. This is accomplished by

The GC Electronic Key Management System (EKMS) was deployed in 2002 to make use of advanced computer technology to provide a secure, automated, responsive and flexible key management system. The GC EKMS relied primarily on technology

Subsequent to the deployment of the GC EKMS, the cryptographic inventory and electronic key management infrastructure. As Canada has traditionally relied on

as was the case with the GC EKMS, many of the issues associated with the

In response, Canada has launched its own Canadian Cryptographic Modernization Program (CCMP), the scope of which includes the modernization of End Cryptographic Units (ECUs) as well as the key management infrastructure (KMI) required to support those ECUs. The key management infrastructure portion of the CCMP is being developed under the Classified Security Management Infrastructure (CSMI) project and along with some other capabilities that have yet to be developed, is referred to in Canada as the GC KMI.

The GC KMI is being developed and deployed in phases and will incorporate those aspects of the that are applicable and necessary to the Canadian operational context. The GC KMI will deliver a modernized key management infrastructure suitable for supporting Canada's High Assurance cryptographic needs for decades to come.

During the next few years, a will be carried out with a key . This will

The final phase of the CSMI project will see access being expanded to include other GC department and agency users.

Users of the GC KMI system, primarily GC department and agency COMSEC custodians, will need to be authenticated before being granted access to the system. GC KMI Users will receive a High Assurance when accessing the GC KMI.

by the GC KMI system.

1.4 Description of the class of records associated with the program or activity

The class of records associated with the personal information collected and stored in the GC KMI are:

Security Class of Record (CoR) [PRN 931]: 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, Royal Canadian Mounted Police, Communications Security Establishment, etc.).

Recruitment and Staffing CoR [PRN 920]: 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.

The personal information being collected by the GC KMI system for authentication and registration of users is covered by the standard Personal Information Banks (PIB) described below:

Identification Cards and Access Badges [PSE 917]: Personal information used in support of physical security and to assist in ensuring the security of government assets present in such facilities. This information is typically collected to register employees for Identification and Building Passes. In GC KMI this information is collected to verify the applicant's identity and security clearance level before granting access to the GC KMI system. Such information may include employee name, Date of Birth (DoB) and security clearance level. This PIB is associated to the CoR [PRN 931].

Personnel Security Screening [PSU 917]: 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), date and place of birth and citizenship status. This PIB is associated to the security CoR [PRN 931] and the Recruitment and Staffing CoR [PRN 920].

1.5 Legal Authority for Program or Activity

The collection, use and disclosure of information are governed by the following Laws, Regulations and Policies:

Laws & Regulations: *National Defence Act, RSC 1987, c N-5, Section 273.64 (1) CSE mandate. Financial Administration Act (FAA), section 7.1.*

Policies: *Policy on Government Security, section 3.9 Departmental Security Management and individual security screening and Appendix B CSE Lead Security Agency Responsibilities.*

1.6 Summary of the project / initiative / change

The GC EKMS was deployed in 2002 to make use of advanced computer technology to provide a secure, automated, responsive and flexible key management system. The GC EKMS relied primarily on technology

cryptographic inventory and key management infrastructure (KMI). In response, and to maintain interoperability Canada has launched the CCMP, the scope of which includes the modernization of End Cryptographic Units (ECUs) as well as the KMI required to support those ECUs. The KMI portion of the CCMP, along with some other capabilities that have yet to be developed, is referred to in Canada as the GC KMI.

Users of the GC KMI system, primarily GC department and agency COMSEC custodians, will need to be authenticated before being granted access to the system. GC KMI users will provide specific personal information so that their identity can be confirmed and they can then be registered as valid GC KMI users. GC KMI Users will receive a High Assurance to be used when accessing the GC KMI.

will be stored
by the GC KMI system.

All user personal information will be fully secured in the GC KMI system and access to the information will be strictly limited and controlled.

2 Risk Identification & Organization

2.1 A: Type of Program or Activity

SECTION II - RISK AREA IDENTIFICATION AND CATEGORIZATION

	Level of Risk to Privacy
Program or activity that does NOT involve a decision about an identifiable individual.	1
Administration of Programs / Activity and Services	2
Personal information is used to make decisions that directly affect the individual (i.e. determining individual authentication and access rights to the system, etc.)	3
Compliance / Regulatory investigations and enforcement	4

Details: Personal information is collected solely for the purpose of registering applicants who require access to the GC KMI in order to carry out the COMSEC roles and responsibilities of their position in their organization. A GC KMI Personnel Registration Form

is required in order to verify the identity and security clearance level before granting access to the GC KMI. This information is entered into the GC KMI system's and stored in the GC KMI

the signed original GC KMI Applicant Agreement Form will be scanned into and stored in the GC KMI system. The applicant's security clearance will be verified by CSE Security staff.

2.2 B: Type of Personal Information Involved and Context

	Level of risk to privacy
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program. For example: general licensing, or renewal of travel documents or identity documents.	1
Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	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.	3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	4

Details: Information is requested for verifying the identity of applicants requesting access to GC KMI and registering them as GC KMI users. Personal information from the GC KMI Personnel Registration Form

signed GC KMI Applicant Agreement Form
are scanned into and securely stored in the

The original

2.3 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

Details: CSE is the lead organization with respect to the GC KMI. Personal information from the GC KMI Personnel Registration Form is entered into the _____ by the GC KMI Personnel Registration Manager (PRM) at CSE. The applicant’s departmental Personnel Local Type 1 Registration Authority (PLT1RA) scans copies of the _____ Human User Agreement Form. The original registration forms are destroyed in an approved classified shredder. The information will only be visible to a limited number of CSE _____ personnel and authorized departmental KMI personnel (refer to section 3.1). No further dissemination of the information will occur.

2.4 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

Details: The GC KMI system is expected to be operational for _____. The operational system will be enhanced as new crypto devices are supported but the user registration database will remain throughout the life of the system. The GC KMI has _____

2.5 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

Details: There are approximately COMSEC accounts for Other Government Departments (OGD) and approximately COMSEC Accounts for DND currently using the GC EKMS. From the GC KMI perspective, this number of accounts (users) is expected to be significantly reduced in DND as a result of Shared Services Canada will use the new Enterprise COMSEC Management and Account model, defined in ITSD-03A Annex B, which will also result in a reduction of the number of OGD COMSEC Accounts. All GC KMI users will be Canadian citizens and Canadian federal government employees.

2.6 E: Technology and 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

The GC KMI will use a new user registration process which will verify applicant's identity, securely store user identification information and when authenticated, will issue users with a and High Assurance for accessing the GC KMI.

2. Does the new or modified program or activity require any modifications to IT legacy systems and / or services? YES
 NO

3. Does 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- YES
 NO

programmable logic).

Please specify:

<p>All registered GC KMI users will receive a High Assurance that is used for accessing the GC KMI. A during registration. No user personal information will be stored on the The user's will not be stored (backed up or archived) by the GC KMI system.</p>

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.

Please specify:

[Empty text box]

- 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 institutions 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 behaviour.

Please specify:

[Empty text box]

- 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

2.7 G: Personal Information Transmission

Level of risk to privacy

The personal information is used within a closed system (i.e., no connections to the Internet, Intranet or any other external system and the circulation of hardcopy documents is strictly controlled). 1

The personal information is used in a 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

Details: Personal information and data will only be transmitted electronically on approved networks, which at the date this PIA was prepared consist of the

High Assurance

The personal information from the GC KMI Personnel Registration Form will be stored in the

Personal information

2.8 H: Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee

Details: Information stored in the GC KMI, based on the GC KMI Personnel Registration Form

The confidentiality of personal information as an asset is rated at PROTECTED

B. The database will be located in the making physical access for non-authorized personnel highly unlikely. Personal information from the Personnel Registration Form will be scanned into and stored in the

In the event of an insider threat, the individual's personal information could be Since all Users and GC KMI staffs are security cleared to a minimum of SECRET and most to TOP SECRET, the

risk of an insider threat would An external breach however would result in an impact as it would

The probability of an external breach due to the robust physical and IT security protection in place for the GC KMI. These risks are in part mitigated by a security awareness program which makes employees aware of what to do if they suspect

In terms of safeguarding the personal information, system access information, IT monitoring, event logging and physical security measures are in place to lower the risk of unauthorized access. Security Screening measures are in place to minimize the risk of insider threat. **The impact of a privacy breach on individuals is assessed as while the risk of this occurring is assessed as**

2.9 I: Potential risk that in the event of a privacy breach, there will be an impact on the institution

Details: The confidentiality of personal information as an asset is rated at PROTECTED B If the

The existing and the stringent IT safeguards reduce the risk of unauthorized access. **The impact of a privacy breach of this nature on the organization is assessed as while the risk of this occurring is assessed as**

3 Analysis of Personal Identification Elements for the Program or Activity

In conducting these activities, CSE and other GC departments and agencies with connections to the GC KMI will comply with their obligations as laid out under the *Privacy Act* with respect to access, use, retention and disclosure of personal information. There is no formal agreement with other departments and agencies on this requirement since all are governed by the *Privacy Act*.

In all cases the information provided will be used solely for GC KMI user authentication and registration purposes. from the table below must be provided during the GC KMI registration process.

The Personal Information elements and sub-elements collected by the GC-KMI system are:

3.1 Acquisition, Storage, Handling and Modification

The GC KMI user personal information will be obtained lawfully through the registration application process. The prospective GC KMI User must willingly provide the requested personal information otherwise no GC KMI access can be granted. At CSE, this information will be stored

Access is accorded only to _____ that have a business requirement and need to know.

Personal information collected and processed during the GC KMI registration process will be handled by the following GC KMI Roles:

Role	Responsibility	Personal information handled
------	----------------	------------------------------

Information can be modified to correct errors on a case by case basis, as authorized by the GC KMI Eligibility Authority, the CSE Personnel Registration Manager or the Personnel Local Type 1 Registration Authority. All users will be re-validated annually using the same process as the original registration. The GC KMI High Assurance will only be issued during the initial user registration.

When users no longer require access to GC KMI due to a change in employment status or responsibilities, their account will be deactivated. Case-by-case deactivations may take place when authorized by the GC KMI responsible authorities listed in the previous paragraph. Personal information will be saved for seven years for audit purposes after which time it will be securely deleted. Retention and disposition of GC KMI Personal Information will be done in accordance with Records Disposition Authority (RDA) No. 2002/011.

4 Flow of Personal Information for the Program or Activity

PLT1RA @ Dept X COMSEC Account	Human @ Dept X COMSEC Account	PRM @ CSE	EA @ Dept X	Human @ Dept X
---	--	-----------	-------------------	-------------------

s.15(1) - DEF

s.16(2)(c)

5 Privacy Compliance Analysis

Collection Authority

The National Defence Act, RSC 1985, c N-5, Section 273.64 (1) (b) states that “the mandate of the Communications Security Establishment is to provide advice and guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada”.

Personal information is collected pursuant to subsection 7.1 of the Financial Administration Act (FAA) and as required under the Policy on Government Security (PGS), section 3.9 Departmental Security Management and Individual Security Screening and Appendix B which states that “CSE as a Lead Security Agency provides leadership and coordination for departmental activities that help ensure the protection of electronic information and systems of importance and serves as the government’s national authority for COMSEC”. At CSE the authority for the collection of the required personal information is delegated to the Chief, CSE.

As the lead GC agency for cryptography, CSE is responsible to provide or approve systems to provide cryptographic materials. CSE is responsible to verify that only authorized individuals can obtain such materials. The GC KMI registration authority will verify the identity of individuals and their authorization to receive such materials.

Notification and Consent

An individual’s personal information, as described in Section 2.1, is collected as part of the GC KMI user registration process, and the individual’s consent is required prior to the commencement of any such collection. This consent is captured by the individual’s completion of the GC KMI Human User Agreement Form,

The signature of the individual attests to their understanding of, and compliance with the *Privacy Act* Notice, which explains the purpose of the collection and the use of the personal information. The individual voluntarily provides
that will be used in the GC KMI registration process.

Accuracy, Use, Retention and Disclosure

User personal information stored in the GC KMI must be accurate and up to date in order to facilitate valid access to the GC KMI system. User personal information entered and stored in the GC KMI system will be retained for seven years. The original GC KMI Human User Agreement Form will be scanned into and stored in the Applicant personal information provided on the GC KMI personnel Registration Form is stored in the The original are destroyed in a classified shredder. User information is re-validated with the registered user, in person, annually following the same process as the initial registration. If the the new documents will be scanned into the GC KMI system. The GC KMI system records the date of the user's registration and subsequent annual updates.

Use of the information will be limited to facilitate access to the GC KMI system, and only by authorized GC KMI Registration staff with the need to know. It will not be disclosed to any persons beyond those individuals.

Administrative, Physical and Technical Safeguards

The information will be collected during the GC KMI User registration process as described in Section IV. Once collected, the information will be entered into the GC KMI system using a High Assurance encryption. The personal information will reside on a classified database in the GC KMI system; to be accessed only by GC KMI authorized personnel.

In addition, a Threat Risk Assessment (TRA) of the GC KMI User Registration process has been completed (Reference: *Threat and Risk Assessment (TRA) In Support of Government of Canada (GC) Key Management Infrastructure (KMI) Registration process, CERRID # 28272690*). This TRA concludes that there are no additional safeguards recommended for the GC KMI Registration Process and that the Residual Risks are rated either

Access to Personal Information

At CSE, access to the personal information exchanged is limited to the staff responsible for managing the GC KMI User registration and access control systems.

This includes:

Detailed descriptions of the GC KMI Roles and Responsibilities can be referenced in the SECRET classified GC CSMI Roles and Responsibilities document (CERRID #10134885).

Limitations on Use

The personal information exchanged will be used solely for GC KMI access control administration purposes (updating and maintaining an access control database of authorized personnel).

Updating Information

The GC KMI User information exchanged must be current and accurate, and will be verified annually. This annual verification ensures that the person's work responsibilities require continued access to the GC KMI and that the personal information is current and valid. Information exchanges for the purpose of updating the relevant information will be handled in a secure fashion as specified in the Information Management section above.

Individual Right of Access

To preserve confidentiality and integrity of the information exchanged, individual right of access is limited to the individual right of access to the GC KMI system.

Compliance Monitoring

Access to the GC KMI system will be monitored and logged to permit review on a regular basis only by the authorized _____ and _____

_____ staff. Anomalies will be investigated immediately and rectified, and/or reported.

In addition, the _____ will monitor the GC KMI for specific security events.

Risk Mitigation

Section II relates the risks to privacy inherent in this program. The GC KMI Registration Process TRA documents the risks posed to the personal information collected and stored during user registration. This TRA determined that all of the Residual Risks for the GC KMI registration process are rated [redacted]. The TRA concludes that there are no additional safeguards recommended for the GC KMI registration process.

The requirement to store GC KMI User's personal information in the GC KMI is dictated by the software components [redacted]. The [redacted] will not have access to any personal information stored in the GC KMI. Storage of access logs for a five year period is mitigated by the physical protection of the server itself, as well as the limited number of personnel with authorized access.

Outstanding Risk Factors

As of the date of this PIA assessment, there may be minor changes to the registration process as the system is implemented and deployed. Changes of significance will be documented in a revised PIA, if necessary.

6 Summary of the Analysis and Recommendations

The very nature of the GC KMI application, to permit authorized users access to the system for ordering device encryption keys, is very secure. All Users must hold at least a SECRET security clearance. The physical, personnel, system and [redacted] High Assurance network security protection in place will ensure that all user personal information will be securely protected.

No additional recommendations are required. Any risks will be satisfactorily mitigated using existing CSE or GC KMI security processes and actions.

7 Supplementary Documents List

- GC CSMI Roles and Responsibilities (CERRID #10134885).
- ITSD-03A, IT Security Directive for the Control of COMSEC Material in the Government of Canada.

Page intentionally blank

8 Formal Approval

I approve this Core PIA and commit to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements as they relate to the administration of this program/ activity.

The Privacy Act, Section 10 delegation is exercised by the Director, Disclosure Policy and Review.


The official accountable for the collection and use of personal information described is the Director General, Cyber Protection, CSE.

The PIA is commensurate with the level of privacy risk associated with the new activity

Joseph Waddington
Director General,
Cyber Protection, CSE

Dominic Rochon
Deputy Chief
Policy and Communications, CSE

* _____ *Adm. UGCIP . 21/06/16*
Signature of official responsible for the Program or Activity /
Date

* 
Signature of Head or Delegate Responsible for administering
Section 10 of the *Privacy Act* / Date

Note: Responsibility for compliance with the requirements of sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage programs and activities are responsible for ensuring that privacy requirements are implemented as part of the administration of the program or activity.

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks, which must be complemented by a Core PIA, and submitted to the Treasury Board of Canada Secretariat.

Page intentionally blank

Appendix A – Sample GC KMI Applicant Registration Forms

Page intentionally blank

s.15(1) - DEF

s.15(1) - IA

s.16(2)(c)

CONFIDENTIAL

s.15(1) - DEF

s.16(2)(c)

CONFIDENTIAL

s.15(1) - DEF

s.15(1) - IA

s.16(2)(c)

CONFIDENTIAL

s.15(1) - DEF

s.16(2)(c)

CONFIDENTIAL