PERSONNEL SECURITY SCREENING SOLUTION (PSS SOLUTION)

Account and case management solution – High-level Business Requirements

Canada Revenue Agency
Finance and Administration Branch
Version 1.02
August 29, 2019

Carpenter, Lynda
Lynda.carpenter@cra-arc.gc.ca

Contents

Approval

NAME, TITLE SECTION DIVISION DIRECTORATE Information Technology Branch	Date
Helena Gorancic-Lazetic, A/Assistant Director Personnel Security Screening Section Personnel Security Screening Division Security and Internal Affairs Directorate Finance and Administration Branch	Date
Marc Jolicoeur, A/Assistant Director Security Risk Assessment Section Personnel Security Screening Division Security and Internal Affairs Directorate Finance and Administration Branch	Date
Bertrand Haubert, Director Personnel Security Screening Division Security and Internal Affairs Directorate Finance and Administration Branch	Date
Dana-Lynn Hills, Director General Security and Internal Affairs Directorate Finance and Administration Branch	Date

1 Introduction

This document outlines the high-level business requirements for a solution to manage accounts, cases and activities for the personnel security screening program.

2 Overview

2.1 Background

In accordance with the Treasury Board Secretariat's (TBS) Standard on Security Screening, a valid security status or security clearance is a condition of employment, contract, appointment or assignment. It may also be established as a condition for other individuals external to government with whom government may need to share or provide access to sensitive or classified information or assets, or access to facilities.

Individuals must obtain and retain a security status or clearance for the period of employment, contract, or agreement. In December 2014, a Personnel Security Screening (PSS) module was released to production in the Corporate Administration System (CAS) to facilitate an online application by employees and the digital processing of security screening requests. This solution also included the ability to manually input requests on behalf of non-employees (i.e. candidates, consultants, contractors).

The PSS module in CAS also provided some functionality to track the activities performed by the PSS user and to record the resulting decision.

During the 2018/19 and 2019/20 fiscal years, some work was started to facilitate the application process for candidates within the Integrated Staffing Solution (ISS). This solution was chosen since it already facilitates an application process with the PSSD client base (external candidates), provides the option to apply the "tell us once" principle as outlined by the One GC philosophy, and most candidates and employees already have a candidate profile created.

This work aligns somewhat with the release of new TBS Security Screening Application and Consent Form which replaces the Security Screening Authorization and Consent Form (TBS/SCT330-23) and the Security Clearance Questionnaire (TBS/SCT330-60).

2.2 Problem statement

In October 2014, TBS released a new Standard on Security Screening (the Standard) which identifies a new type of security screening and has influenced changes in the way security screening is being processed, including the activities performed during the assessment phase of a security screening request.

In January 2016, the Canada Revenue Agency (CRA) Personnel Security Screening Division (PSSD) reassessed its way of doing business as it relates to processing requests for security screening. PSSD chose to partially de-centralize their process and distribute some of the screening activities to security personnel located at the local offices through the regions rather than maintain all activities in Headquarters.

In addition, the PSS module in CAS was released to production in December 2014 as a minimal viable product focused on supporting a single team rather than a distributed workforce with differing responsibilities, with the intention of adding further functionality to address other needed workflows and automations. Due to development constraints and changes brought forward by the release of the new Standard and the new structure associated to PSS processes, the additional functionalities have yet to be addressed and prove to be continued challenges.

This document will serve as a guide to outline the present needs and to assess a possible future solution's fit to these requirements.

2.3 Proposal and scope

The proposal is to have a solution that allows for:

- an individual to request a security screening assessment online, regardless of the individual being an external candidate, a contractor, an internal employee, or another individual who requires access to sensitive or classified information or assets, or access to facilities
- the processing of a security screening application
- the maintenance of an individual's security screening file
- the confirmation of an individual security screening status at a quick glance

The solution must be able to provide a global view of an account with its associated cases and activities. The global view of the account must be able to tell the approved user the status of the account.

For the purposes of this document, an account is unique to an individual and may contain several cases which are unique to a specific security screening application or aftercare review, and within each case, one or more activities may exist which are specific to a type of validation or event or action taken.

2.4 Benefits

Providing the means for applicants to key in their information themselves has the potential to:

- Eliminate the need for data entry by security screening staff
- Decrease the number of typing and interpretation errors while entering data from security screening application forms
- Allow for security screening staff to focus on the process instead of the data entry

Introducing some automation has the potential to:

- Increase efficiencies in the processing of security screening
- Allow for security screening staff to focus on the analysis portion of the process
- Ensure appropriate data to managers to assess trends associated to the security screening business needs

Ensuring interconnectivities with key systems has the potential to:

- Provide near real-time data is available to key stakeholders
- Increase efficiency in the transmission of data with service providers and partners

2.5 Statistics

The CRA processes on average 80,000 staffing actions a year. Given that security screening is a condition of employment in accordance with the Standard, each of those staffing actions requires an action by security screening, from confirming the validity of a security screening status, whether within the Agency or with another Government of Canada institution, to processing a new, update, or upgrade request in order to support the staffing action.

As a result of staffing actions, PSSD processes, on average:

- 7,428 transactions per year associated to external candidates

- 4,078 transactions per year associated to internal employees who require an update to their security screening status
- 928 transactions per year associated to an upgrade of security screening statuses
- 1579 transactions per year associated to confirming security screening statuses with other Government of Canada institutions and following up with requesting the status be transferred to CRA

In addition to the above mentioned transactions associated to staffing actions, the PSSD also processes, on average:

- 367 transactions per year associated to transferring security statuses to other Government of Canada institutions
    - Note: This does not include the number of confirmations of security screening statuses to other Government of Canada institutions
- 760 transactions per year associated to downgrading security screening statuses to match the requirements of the position held by employees
- 298 transactions per year associated to assessing the impact of new information provided by employees on their security screening status

This represents a total of an average of 13,859 transactions per year related to security screening activities.

2.6 Assumptions, risks and dependencies

The successful completion of this project is dependent on the following:

- Resource availability in HRB
- Resource availability in ITB
- Resource availability in PSSD
- Resource availability in OGD where impacted or required such as with SSC or with RCMP or with CSIS as these other organizations are involved with certain mandated actions
- The implementation of these changes must be coordinated with Security assessment and production assurance teams
- The implementation of these changes must be coordinated with CAS and ISS functional and technical support teams
- Available funds for development, licenses and maintenance
- The integrity of technical changes resulting from other stakeholders/partners such as, but not limited to:
    - CSIS – updating their system to accept new data identified by the new Security Screening Application and Consent form from TBS
    - RCMP – changes within their Real-Time Identification (RTID) solution and/or within their SIBS team for Law Enforcement Records Check (LERC) verifications
    - TBS – any further changes to the new Security Screening Application and Consent form

2.7 Contingency plan

The following options would be considered if a new solution cannot be found to meet the needs of the PSSD:

- Continue to work with (CESD) to maintain the current solution within CAS until it is no longer supported in 2025
- Migrate to the new HANA SAP platform which means an architectural constraint on data management and increased in expense
- Revert back to using the MS Access database and a paper based process. Of note is that there is no longer the ability to modify or configure this solution

- Create new MS Access clone with potential of missing functionality. Of note that this would require a variance and would be considered a stop-gap solution only
- Outsource the security screening program

2.8 Impacts

- Procedures available via Management Hub, Know How and the Security site will need to be updated
- System documents and training materials are likely to need to be replaced
- A communication strategy needs to be established to disseminate information related to the project

3 Role requirements

Existing solution was designed with a single user type in mind. The security screening program has since been de-centralized to a degree and it is recognized that it requires consideration to multiple user types and communities.

3.1 User types

Applicant user: This type of user requires access for the sole purpose of supplying information to the system for the assessment of their security screening status. They will typically complete a "form" which would lay out the required information to be collected associated to the level of security screening required and capture electronic signatures as required thus permitting the Security screening and PSS users to process the request.

HR/Staffing user: This type of user requires access for the sole purpose of validating an individual's security screening status. This may require the HR/Staffing user to reach out to the PSSD to initiate a validation with another Government of Canada institution. This type of user might also be called upon to provide a confirmation that certain activities that are common to both suitability and security have been done.

Other security user: This type of user typically validates an individual's security screening status for the purpose of issuing an ID/Access card. This type of user may also contact PSSD to initiate a validation with another Government of Canada institution.

Security screening user: This type of user typically initiates the security screening process. Where required, they currently receive paper copy forms for external candidates and enter the data into the system. They will also capture fingerprints and send them to the RCMP via the RTID system. They will pull the credit report from the Equifax (current process) web service, save a copy of the report and populate a credit matrix which provides a pre-risk assessment associated credit. In addition, this type of user will coordinate the security briefing with the employee.

Supervisor user: This type of user is typically a regional security manager or regional security specialist. They work closely with statistics associated to their specific area of responsibility. They are responsible for the work of their direct reports in the Security screening user group.

PSS user: This type of user takes over the processing from the Security screening user. They will receive the results from the fingerprints verification via the RTID system, save a copy and note the result. They will review the credit matrix and report. As required, depending upon level of screening, they will forward the request to CSIS for the security assessment and receive the results in accordance with CSIS service standards. If little to no security risks, as per set parameters, they will render the decision to grant or maintain the security screening. They will issue a security briefing form to be completed by the employee via the Security screening user.

SRAS user: This type of user reviews complex cases. These can be those that have significant risks, in accordance with set parameters, and which were referred by the PSS user during normal processes. They may also be identified outside of normal process, such as when an investigation was initiated by the Internal Affairs and Fraud Control Division, self-reported by employee, or reported by third party. These individuals will perform any and all activities deemed necessary to assess the risks associated to the adverse information and works with templates to notify stakeholders of actions being taken and the decisions associated to the assessment.

Management user: This type of user is responsible for the PSS program. They work closely with statistics and have approval roles in the decision making process, especially in complex cases. They are also responsible to ensure the appropriate staff is in place for the workload.

ASO user: This user is the Agency Security Officer and Director General of the SIAD. The ASO is responsible for the decisions made within the security screening program and may be called upon in circumstances to approve a decision.

Business Support user: This type of user is responsible to ensure that all systems are functioning as intended. They will provide some troubleshooting support to all other users. They will also initiate any change requests that are required. They will also assist management with complex reporting needs.

Technical user: This type of user is also responsible to ensure that all systems are functioning as intended but has added responsibility to identify and address changes stemming from other activities in the environment where the solution resides such as changes related to modifications by others in sources where this solution draws certain data from. E.g. a system change in some table that is outside this solution but that this solution requires to read data from in order to function. Note: there may be more than one type of technical user required.

Audit / quality assurance user: This type of user will view the full account(s) to ensure compliance with the TBS Standard on Security Screening, the CRA Directive on Personnel Security Screening, and the processes in place, to name a few. They would not need to make any modifications to the accounts viewed.

3.2 Technical considerations

- The ability to assign multiple user types to a single user
- The ability to assign user types on ad-hoc, short-term basis as required
- Synchronisation of identification particulars with corporate ID management (IAM)
- An order is to be established amongst the functionalities within the user type groupings

4 Business requirements

4.1 Account management

4.1.1 Summary

The PSSD view its data holdings as files, from this point on referred to as “account”. Each account contains requests, from this point on referred to as “case”. The decisions associated to each case influences the account’s status. Some decisions, such as cancelling a security screening status, is an overarching decision for the account. When data needs to be transferred to other Government of Canada institutions , it is all data and decisions associated to the account that is transferred, with a few exceptions. Therefore, there is a need for users to view and manage an account holistically.

4.1.2 Basic details

Actors:	HR/Staffing user (only for requirements M-AM-01 and M-AM-02); Other security user (only for requirements M-AM-01 to M-AM-03); Security screening user; PSS user; SRAS user; Management user
Triggers:	A need to confirm the existence and status, level and validity of a security screening account, either ➢ prior to creating a new case (avoidance of duplication) ➢ prior to committing to a staffing action ➢ following a request from another Government of Canada institution to confirm, which is usually followed by a request to transfer
Pre-conditions:	The existence of an account having been created, usually associated to an initial case launch

4.1.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-AM-01	The solution must present the user with a holistic view of the account.		
M-AM-02	The solution must present a summary of the account security screening status based on a logic mapping associated to varying combinations of decisions rendered within the cases associated to the account. This would include, at a minimum: ➢ Selected tombstone data to identify the subject of the account ➢ status (active, inactive) ➢ if a case is in progress ➢ level ➢ validity period		
M-AM-03	The solution must present, at a minimum, the following information: ➢ some basic employment and/or candidate information as per CAS (CRA data only) or ISS data, including: o employment/candidate status (active, inactive, withdrawn, student, interchange, etc)		

	○ date on-boarded ○ date off-boarded ○ reason for departure (only viewable by PSS, SRAS, and Management users) ➢ some basic position and/or staffing action as per CAS or ISS data, including: ○ position title ○ position number and/or requisition number ○ security requirement ➢ some basic contract information where applicable, including: ○ contract number ○ contract dates/duration Note: contractors may be associated to 0 to many contracts which would need to be displayed.		
M-AM-04	The solution must present retention period information as per the calculations described in requirement M-DM-02: ➢ date account became inactive ➢ date retention period is met		
M-AM-05	The solution must present any account level comments.		
M-AM-06	All data presented about the account except for M-AM-05 is viewable only. The solution must allow designated user groups to add comments.		
M-AM-07	The solution must present the list of cases associated with the account and include a display of the following information (at a minimum): ➢ Case number ➢ Case status ➢ Decision rendered ➢ Date of decision		
M-AM-08	The solution must allow specified users to access any case listed considering the following condition: ➢ A closed case must be viewable only ○ Exception: support and technical users must be able to modify a closed case ➢ Specified users must be able to choose to view only or modify an active case. Consideration to be made for restricted access based on geo-location, activity based, work assignment, etc.		

Enhanced criteria		Possible Yes/No	Comments
E-AM-01	Enhanced criteria related to requirement M-AM-03 when displaying information about a contractor. The solution should include the contract security requirement.		

4.2 Search functionality

4.2.1 Summary

Users will need to search for accounts and/or cases. Once results are returned, they may require to take one or more actions, some following a submission by the applicant user, and in other situations, to initiate a case within an account.

4.2.2 Basic details

Actors:	All users
Triggers:	None
Pre-conditions:	None

4.2.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-SF-01	The solution must allow a user to search by several criteria markers individually or together. Examples of criteria: ➢ Given and/or surname ➢ Date of birth ➢ Case number ➢ Account number ➢ PRI and/or candidate number ➢ Contract number ➢ Company name (for contractors)		
M-SF-02	The solution must allow the use of typical wildcard characters such as the asterisk (*) and question mark (?) within the search criteria.		
M-SF-03	The solution must look to all related fields to the search criteria entered. For example, if last name is entered, the solution will search all surname fields for a return on results.		
M-SF-04	The solution must return account level results. Essentially one result per account that matches the search criteria, regardless of the number of cases for the account.		
M-SF-05	The solution must include, at a minimum, the following output: ➢ Account number ➢ All names (given and surname) ➢ PRI and/or candidate number ➢ Number of cases associated to the account		

	➢ If any cases are active		
M-SF-06	When using contract number or company name as search criteria, the solution must return all accounts associated to the contract number or company		

Enhanced criteria		Possible Yes/No	Comments
E-SF-01	The solution should provide a means by which the user can refine their original search criteria on the original search outcome.		
E-SF-02	The solution should allow the user to return to their last search outcome following the access of an account accessed in error.		

4.3 Workload management

4.3.1 Summary

Users must be able to manage their workloads and address take actions efficiently as required.

4.3.2 Basic details

Actors:	Security screening user; PSS user; SRAS user;
Triggers:	Track cases assigned to them that require activities to take place
Pre-conditions:	Cases are in process

4.3.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-WM-01	The solution must present the user with a dashboard reflective of cases in process and allows the user access to those cases for viewing and modifying, based on roles and permissions.		
M-WM-02	The solution must present lists, based on permissions and be customized by the user, for, at a minimum, the following situations: ➢ Full list of cases in process ➢ Cases in process assigned to a specific user ➢ Cases in process assigned to specific groups ➢ BF alerts		
M-WM-03	The solution must allow the user to access and modify cases as required.		
M-WM-04	The solution must restrict access as required when already in use by another individual – lock-out feature.		
M-WM-05	The solution must manage level of access (view only or modify) to case.		

M-WM-06	The solution must allow the user to initiate an application on behalf of an applicant user.		
M-WM-07	The solution must allow the manager user to restrict access to accounts or cases for specified user or user groups as required and based on sensitivity of case/account.		

4.4 Applicant experience

4.4.1 Summary

Most cases are initiated by the need to apply for a security screening status, whether as part of a staffing process or a cyclical update. This activity is done by the following types of individuals:

- Internal employees
- External candidates
- Internal candidates
- Contractors and consultants
- Other individuals who are not considered employees of the Agency but have a need to access CRA sensitive information, assets or facilities

In addition, employees, contractors and consultants, and other individuals are expected to report changes in personal circumstances or other concerns to their security screening status during the lifecycle of their account. They are to report these changes regardless of the cyclical updates.

4.4.2 Basic details

Actors:	Applicant users
Triggers:	A final step in the staffing process or a cyclical update
Pre-conditions:	Accessible external and internal to the Agency

4.4.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-AE-01	The solution must present the user with the fields defined by the TBS Security Screening Application and Consent Form and designed by the CRA to enhance and simplify the completion processes such as control mechanisms.		
M-AE-02	The solution must be interactive with the user, presenting only fields required by the level identified and based on selections made by the user		
M-AE-03	The solution must validate the data entered for completeness and compliance		
M-AE-04	The solution must capture electronic signatures		
M-AE-05	The solution must present the required feels of the TBS application to the candidate for completion only once the HR staffing process has reached a certain stage and a decision has been rendered to require completion.		

M-AE-06	The solution must prevent a user from applying for a cyclical update unless certain conditions are met.		
M-AE-07	The solution must have the application available to employees, contractors, consultants and other individuals at all times for reporting of changes.		
M-AE-08	The solution must allow for the users to access a summarized view of their security screening profile, including approved actions that they may take on their security screening account (cyclical update, reporting changes, etc)		
M-AE-09	The users must be able to save an incomplete application should they need to research required information		
M-AE-10	An incomplete application should remain available for a pre-defined period of time with the user only needing to resave to prolong the period.		
M-AE-11	The solution must be able to retrieve data from a previous application and present it to the user for confirmation, validation and updating as required. This could be the most current prior application or an older dependent on content required by the user. For example, the applicant has a secret clearance, then a reliability status, and now needs secret again. The solution would bring forward the data from last secret where not contained or overwritten in the current reliability. A first security screening application (usually external candidates), the solution must be able to retrieve common data and attachments, from the HR/staffing systems. See requirement M-SA-06 for details about attachments previously provided to HR/Staffing systems.		
M-AE-12	The solution must validate the level of screening requested with the level required by the position. If not a match, the solution must initiate a justification process by the individual's management (or hiring manager). Note: an exception rule would need to be identified to address when a grouping of positions were identified for upgrade in security but not yet identified in the HR systems (for example: ITB positions).		

M-AE-13	The solution must allow the user to view previously submitted applications.		
M-AE-14	The solution must present a summary of all cases associated to their account with the following information, at a minimum, displayed: ➢ Case # ➢ Date submitted ➢ Date completed ➢ Status of their case		
M-AE-15	The solution must accept attachments to be associated to the case and/or to a specific activity within the case and or specific activity within the account for the individual.		
M-AE-16	Where the applicant is less than 18 years old, the solution must provide for a prescribed attachment with the parent or guardian's signature. The solution must recognize the presence of this attachment to release the application to the next step. An associated enhanced criteria is detailed in E-AE-01.		
M-AE-17	The solution must return a confirmation notice upon successful submission of their application.		

Enhanced criteria		Possible Yes/No	Comments
E-AE-01	The solution should be able provide a means to allow a parent or guardian to sign off where the applicant is less than 18 years old. If this is not possible, a counter requirement is listed in section at M-AE-17.		
E-AE-02	The solution should provide the users with the means to arrange their fingerprinting appointment, as required. Note: Fingerprints are mandatory when no fingerprints are logged on the account or when the fingerprints taken are too old (TBD).		
E-AE-03	In order to follow the latest technology standards at the CRA, the solution must be fully compatible with tactile surfaces. The system is expected to be fully usable on tablets and touchscreen monitors. The solution is not expected to be used on Blackberry and other mobile phones.		
E-AE-04	The solution must also be fully capable of accepting keyboard input equivalents to mouse actions. This means the use of the enter key		

	and cursor arrows as well as use of mouse click to press any "button" presented on-screen.		

4.5 Security screening activities

4.5.1 Summary

The Standard on Security Screening details the minimum security screening activities to be performed based on level of security screening requested which would appropriately provide a meaningful assessment of an individual's reliability and/or loyalty as it relates to that reliability. This section will provide the requirements of a solution as it relates to those activities.

4.5.2 Basic details

Actors:	HR/Staffing users (only for requirements M-SA-01 to M-SA-06); Security screening users (only for requirements M-SA-02 and M-SA-07); PSS users; SRAS analysts Note: Unless otherwise stated, these requirements are hidden from the HR/Staffing users
Triggers:	New case creation or adverse information reported to SRAS
Pre-conditions:	Level of screening required is defined

4.5.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-SA-01	The solution must allow the user type = HR/Staffing to identify the background information that was verified and log a summary		
M-SA-02	The solution must allow the users (including HR/Staffing user) to log the ID seen and validated		
M-SA-03	The solution must flag any time outside of Canada found within the residence section of the application form		
M-SA-04	The solution must allow the user type = HR/Staffing to identify the education and professional credentials verified and detail how they were verified (example, did they call the institution to validate?)		
M-SA-05	The solution must allow the user type = HR/Staffing to identify the personal and/or professional references that were contacted and complete a questionnaire associated to security concerns		
M-SA-06	The solution must allow the user type = HR/Staffing to transfer, or allow a view of, documents (such as proof of citizenship, educational/professional background)		
M-SA-07	The solution must allow the user types = security screening and PSS to perform actions detailed in requirements M-SA-01 to M-SA-06 as well and as additional entries		

M-SA-08	The solution must allow the user to release the application back to the applicant in a modifiable format. This release of the application must include user-driven instructions. Note: This is to allow the collection of additional information as required.		
M-SA-09	The solution must allow the user to attach a copy of the credit workbook (excel document) and log the result. (See requirement E-SA-04 and E-SA-05 for enhanced criteria)		
M-SA-10	The solution must provide a space where the user can log the results for the criminal record check. (See requirement E-SA-02 and E-SA-03 for enhanced criteria)		
M-SA-11	The solution must be able to exchange data with the SIBS program at RCMP in a prescribed format and protected (encrypted) as specified by RCMP.		
M-SA-12	The solution must be able to exchange data with CSIS in a prescribed format and protected (encrypted) as specified by CSIS.		
M-SA-13	The solution must allow the SRAS user to diarize the findings associated to open source inquiry and reveal only the summary results (negative or positive) to specified user groups.		
M-SA-14	The solution must allow for other activities to be addressed for which the process and providers are yet to be determined. These include: ➢ Foreign assets ➢ Military service ➢ Polygraph examinations		
M-SA-15	The solution must be able to facilitate the use of templates. For example, templates would be required for (not limited to): ➢ Security questionnaire ➢ Security interview questions ➢ Personal/professional references questionnaire ➢ Security risk assessment (Pre and Final) ➢ Letters of notification		
M-SA-16	The solution must manage the completion and approval process associated to each template and specified activities		
M-SA-17	The solution must facilitate the user to view data points that have changed across cases (comparison with previous application), as applicable, and other key data elements.		

Enhanced criteria		Possible Yes/No	Comments
E-SA-01	The solution should manage a scheduling calendar both at a nationwide level and at an office specific level.		
E-SA-02	The solution should be approved for use on the RTID computers		
E-SA-03	The solution should be able to receive the RCMP fingerprint results directly from the RTID store and forward server		
E-SA-04	The solution should be able to exchange data with the credit reporting company(ies) web service, both feeding tombstone data and capturing the results from said web service		
E-SA-05	The solution should be able to provide the PSS and SRAS users with an analysis of the data from the credit reporting company(ies) based on set parameters/thresholds		
E-SA-06	The solution should manage combination of priority and location based case assignment		

4.6 Exceptions for contractors

4.6.1 Summary

Contractors and consultants are screened with the normal validity period prescribed by the TBS Standard on Security Screening however, CRA sets the validity period to align with the contract period which is extensible until the end of the prescribed period of time, at which time a cyclical update is required.

4.6.2 Basic details

Actors:	PSS users
Triggers:	Receive notification from Contracting that a contract has been extended.
Pre-conditions:	Contracting has: ➢ Provided a list of associated contractors to the extension ➢ Each contractor listed has an account Note: Some contractors may need to update their security screening account or apply for security screening as part of this activity.

4.6.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-EC-01	The solution must allow for a bulk account level activity to update the following information: ➢ Contract number ➢ Company name ➢ Validity period		
M-EC-02	The solution must identify when a natural validity period based on Standard on Security Screening prescribed validity periods is		

	surpassed by the bulk activity identified in M-EC-01.		

4.7 Exceptions for review for cause

4.8.1 Summary

Review for cause (and resolution of doubt for external applicants and upgrades) is a ad-hoc process when additional information is provided to PSSD by various sources that may influence the risks associated to maintaining (or granting) a security screening to an individual. This process may also be independent of a specific screening application process and therefore must have an ability to review the entire account for the individual.

4.8.2 Basic details

Actors:	SRAS users; Management users;
Triggers:	➢ Adverse information was discovered as part of the screening activities listed in section 4.5 during an initial security screening or an upgrade ➢ Adverse information was provided to PSSD that could affect an individual's security screening status
Pre-conditions:	

4.8.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-RfC-01	The solution must allow the user to launch a new case		
M-RfC-02	The solution must provide space for the user to enter pre-defined data, some mandatory, some optional.		
M-RfC-03	The solution must allow for approval workflows with individuals in PSSD and outside PSSD		
M-RfC-04	The solution must allow the user to identify the screening activities required to assess the information provided		
M-RfC-05	The solution must restrict viewing and modification access to portions of this type of access based on pre-defined parameters		

Enhanced criteria		Possible Yes/No	Comments
E-RfC-01	The solution should provide a connectivity with EFMS solution for transfer of specified data from IAFCD for the purpose of launching a new case to manage review for cause process		
E-RfC-02	The solution should provide a means by which employees can report: ➢ Changes in behaviour ➢ Changes in circumstances ➢ Contact or incident reports		

	And this on behalf of themselves or about others (reference: Standard on Security Screening, Appendix F, Sections 7 to 9)		
E-RfC-03	The solution should facilitate scheduling key events within the process		

4.8 Data management

4.8.1 Summary

PSSD is mandated by the TBS Standard on Security Screening to retain a security screening account for a minimum of 2 years following the last administrative action on file. This retention period is 10 years when a negative decision has been rendered on the file.

CRA has decided that it will retain a security screening account for a minimum of 3 years except when adverse information is present on file in which case it will be retained for 10 years following last administrative action (decision associated to the account becoming inactive).

4.8.2 Basic details

Actors:	PSS users
Triggers:	Individual has: ➢ Not been hired within 1 year following initial security screening assessment (1st case introduced to the account) ➢ Left the CRA
Pre-conditions:	The existence of the individual's account

4.8.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-DM-01	In conjunction with HR systems, the solution must automate a departure process which in turn cancels (renders dormant-closed) an individual account		
M-DM-02	The solution must calculate the required retention period based on certain data being present within cases or the account overall. Note: the calculation will vary dependent upon presence of other data. If adverse information is noted as present 10 years, if no adverse noted 3 years, if confirmation only 1 year. Number of years per condition set subject to change and must be modifiable by a designated user group. Note that subsequent actions on file may extend or annul the retention periods from the account, depending on the actions taken. Examples include: ➢ ATIP request would extend ➢ New case initiation is likely to annul, depending on the case		

M-DM-03	The solution must display the date of cancellation (close-out) and the expected end of retention date		
M-DM-04	The solution must prompt the users when retention dates have passed		
M-DM-05	Upon approval from users, the solution must purge all data, with the exception of tombstone data (TBD), from the solution		
M-DM-06	The solution must allow PSS users to reactivate an account when conditions are met.		
M-DM-07	Upon reactivation, the solution removes retention dates.		

Enhanced criteria		Possible Yes/No	Comments
E-DM-01	The solution should include a workflow to address the security debrief upon employee departure from the CRA		
E-DM-02	The solution should allow users to see if the individual has moved to an OGD – specify the OGD where available (if data is available in HR systems). Override by user must be possible.		
E-DM-03	In conjunction with requirement E-DM-02, the user should be able to note if the OGD was contacted prior to account purge		

4.9 Transferability

4.8.1 Summary

In addition to the retention periods, security screening files are transferable between departments in the case of employee movement. Therefore, there is a need to make accounts, along with all evidentiary data and documents (including e-signatures), available to the other government departments.

The same is true when an employee moves to the CRA. Therefore, there is a need to log a confirmation received from an OGD followed by creating a case reflective of the data and evidentiary documentation received from the OGD.

4.9.2 Basic details

Actors:	HR/Staffing users; PSS users
Triggers:	➢ Request from OGD to confirm followed by request to transfer the file ➢ Request received from HR/Staffing user to confirm with OGD followed by confirmation that individual is hired
Pre-conditions:	Interoperability with HR/Staffing systems.

4.9.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-T-01	The solution must allow the HR/Staffing user to request a confirmation from an OGD		

M-T-02	The solution must allow the PSS user to enter basic information about the OGD security screening status, including the period for which PSSD on behalf of the CRA will honour the confirmation (retention period)		
M-T-03	The solution must detect when the individual is on-boarded and prompt the PSS user to request the file transfer from OGD		
M-T-04	The solution must allow the PSS user to identify when the file from the OGD has been received and attach documentation		
M-T-05	The solution must allow the PSS user to perform screening activities as per section 4.5 as required with a means by which the PSS user can indicate why they are performing the screening activities (i.e. evidence not on file received, last verification done more than 5 years prior, etc)		
M-T-06	The solution must allow space where the PSS user can enter OGD names that have requested confirmations (account level) – viewable only be PSS users		
M-T-07	The solution must allow for the transfer of all data and evidentiary documentation, including evidence of e-signatures, to an OGD Note: there may be a need for multiple formats depending on the receiving OGD requirements.		
M-T-08	The solution must allow for the PSS user to select the data to include/exclude in the transfer package.		
M-T-09	The solution must allow data and documents to be attached to an encrypted email for transmittal to the OGD. Note: This requirement is based on current option. To be discussed if other mechanisms are available to address this requirement		
M-T-10	The solution must reflect the account as inactive due to transfer out and set retention period for one year following transfer.		

4.10 Reporting

4.10.1 Summary

Reporting is an essential part of managing a program and ensuring Standard Level Agreements (SLA) are met.

4.10.2 Basic details

Actors:	All users

Triggers:	Assessing program efficiency
Pre-conditions:	Various

4.10.3 Criteria

Mandatory criteria		Possible Yes/No	Comments
M-R-01	The solution must provide reporting capabilities in accordance with business days and factor in statutory holidays and CRA union agreements		
M-R-02	The solution must allow for pre-determined scheduled reporting and provided to users based on roles		
M-R-03	The solution must allow for ad-hoc, manual reporting		
M-R-04	The solution must allow for role based restrictions on ad-hoc reporting		

Enhanced criteria		Possible Yes/No	Comments
E-R-01	The solution should allow for specified user groups to add scheduled reports as required		

5 Functional requirements

Mandatory criteria		Possible Yes/No	Comments
M-FR-01	The solution must manage a BF system, both at a case level and at an activity level.		
M-FR-02	Related requirement to M-FR-01 and reports: A business day calculation must be present to be added into report/dashboard views but the user must not be restricted to determining BF solely by business day period and can rely on day of week for setting BF date.		
M-FR-03	The solution must be able to ensure data entry is consistent (all caps, ascii characters, etc). Note: the detailed requirement for this will be dictated by CSIS and/or RCMP		
M-FR-04	The solution must be capable of automating certain activities and workflows such as, but not limited to: ➢ Initiating cyclical updates ➢ Capturing managerial justifications for upgrades above position requirements ➢ Security briefing		

	➢ Receipt of results from RCMP (RTID* and LERC) and/or CSIS ➢ Pulling credit reports* ➢ Others where identified during development Note: activities and workflows listed with an asterisk (*) are considered enhanced criteria as identified in the Enhanced criteria table in section 4.5.		
M-FR-05	The solution must interoperate with the staffing and HR solutions where security requirements for positions and processes will be set, thus driving the form to be completed by the applicant (Section 4.3) among other requirements, whether identified in the above business requirements and/or identified during the development phase of this project		
M-FR-06	The solution must make the application portion of the solution (as described in section 4.4) accessible by individuals external to CRA via a secured interface with credential management so the individual who accesses the service is established and known and the data is protected.		
M-FR-07	In conjunction with HR systems, the solution must automate a departure process which in turn cancels (renders dormant-closed) an individual account		
M-FR-08	The solution must audit all actions taken within security screening accounts and cases, including when an account or case was only viewed by a user Requirement to write to the audit trail mechanism that the CRA uses is to be discussed with IAFCD and ISD.		
M-FR-09	The solution must be certified for Protected B classification and allow for an identifier when something at a higher classification is stored outside the solution infrastructure		
M-FR-10	The solution must capture user e-signatures as required by different processes		
M-FR-11	The solution must allow for ad-hoc reviews of accounts. Consideration: Report from solution identifying accounts to be reviewed based on pre-defined parameters – solution could create case on behalf of users or users create cases when they initiate the review		

M-FR-12	The solution must have multiple means for data ingestion, conversion, archiving, and exportation. Required formats are to be determined. Volume for historic ingestion and conversion is to be determined.		

Enhanced criteria		Possible Yes/No	Comments
E-FR-01	The solution should allow for a training environment for new users		
E-FR-02	The solution should allow different user groups to communicate with each other		
E-FR-03	The solution should interoperate with AIS		

6 Document Management requirements

Document management for the purposes of personnel security screening program refers to an ability to associate any physical and/or electronic item or object that is not in and of itself a formal part of the solution. Such items/objects may be emails received or sent, paper or scanned documentation such as the TBS application, photocopy of a birth certificate, divorce decree, letter of good conduct, list of individuals under a specific contract, etc. While direct storage of these items/objects within the solution itself is preferred, the ability to associate each item/object to one or more accounts and cases within the solution depending upon the separate repository security and non-repudiation capabilities may be acceptable.

It is considered that based upon current understanding of the restrictions imposed upon the "corporate repository" options available to the CRA that more than one of these would be required to address the program needs. For example "documents" are received and sent from and to external sources, received and sent from and to internal sources. Some are encrypted, some are not. Some may be shared, some not. Multiple formats also apply.

Mandatory criteria		Possible Yes/No	Comments
M-Doc-01	The solution must provide an ability to record the existence of a "document" at each of the following levels: (may not be a complete list) ➢ Account ➢ Case ➢ Activity/task		
M-Doc-02	The solution must provide the ability to retrieve the "document" from within the solution and to display the details. Note: both display of the document metadata details and display of the content of the "document" is required.		
M-Doc-03	The solution must allow the user to "attach" a "document" to any of the above noted levels within the solution.		
M-Doc-04	The solution must allow the user to "link out to" (provide a hyperlink) both "documents" and		

	"web references (URL)" at any of the above noted levels within the solution.		
M-Doc-05	The solution must allow the user to create a friendly (alternative) name for the document or link that does not overwrite the actual file name or full address of a link.		
M-Doc-06	The solution must provide the ability to list all documents associated to an account and show the time of association (sorted in order) and the identity of who uploaded or referenced the item.		
M-Doc-07	The solution must provide a means to turn the account, case, or activity/task into a document that can be "saved" to a repository of the users' choice. (local drive, corporate repository, etc.).		

Enhanced criteria		Possible Yes/No	Comments

Appendix A – Definitions

Applicant:

An individual who is initiating a request on their own security screening account. This may include:

- Internal employees and candidates
- External candidates
- Contractors
- Other individuals who may require access to sensitive information, assets or facilities

Security screening file:

A grouping of security screening requests and associated events kept together either in a physical filing system or in a digital format on a network drive. There should only be one file per applicant. This would be the equivalent of an account.

Request:

An application submitted and processed to issue a decision. This would be the equivalent to a case.

Active case:

A case that is currently being processed.

Closed case:

A case for which the process has been completed and a decision rendered.

Active account:

An account where at least one associated case is in a state where processing is either not finalized or where the validity period of the security screening has not yet expired.

Inactive account:

An account that has been cancelled, suspended, on hold, revoked, and when an initial screening request or, sometimes, when a security screening request to upgrade the level is denied.

Note:

- Cancelled is the only action that is taken outside of a case type scenario that would render an account inactive.
- Suspended and on hold are actions that are taken within a case that would render the account temporarily inactive.
    - Suspending a security screening status is typically done while completing a review for cause case
    - On hold is typically applied when a security screening process is unable to continue while the employee is on a leave of absence
- Revoked and denied are decisions that are rendered at the case level that would render the account inactive.