Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Standard on Security Screening

Published: Oct 20, 2014

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-27/2014E-PDF
ISBN: 978-0-660-20377-5

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Norme sur le filtrage de sécurité

Standard on Security Screening

1. Effective date

1.1 The *Standard on Security Screening* (this Standard) takes effect on October 20, 2014.

1.2 It replaces the *Personnel Security Standard* dated June 9, 1994 and all mandatory requirements contained in security policy implementation notices (SPINs) up to the effective date of this Standard.

1.3 Security screening forms issued by the Treasury Board of Canada Secretariat will be used by departments and agencies for the collection, use, disclosure, retention, and disposal of personal information for the purpose of security screening in accordance with this Standard.

1.4 Departments and agencies have up to 36 months from the effective date to fully comply with all requirements in the Standard, in accordance with the Treasury Board of Canada Secretariat implementation plan.

2. Application

2.1 This Standard applies to all departments as defined in section 2 and any other agency included in Schedules IV and V of the *Financial Administration Act* (FAA), unless excluded by specific acts, regulations or orders-in-council.

2.2 Agencies and Crown corporations can enter into agreements with the Treasury Board of Canada Secretariat to adopt the requirements of this Standard and apply them to their organization. Previous arrangements entered into by agencies and Crown corporations remain in effect.

2.3 Sections 7.4 and 8.0 relating to the role of the Treasury Board of Canada Secretariat in monitoring compliance and consequences for non-compliance do not apply with respect to the following:

- The Office of the Auditor General,
- The Office of the Privacy Commissioner,
- The Office of the Information Commissioner,
- The Office of the Chief Electoral Officer,
- The Office of the Commissioner of Lobbying,
- The Office of the Commissioner of Official Languages,
- The Office of the Public Sector Integrity Commissioner, and
- Agencies and Crown corporations that enter into an agreement with the Treasury Board of Canada Secretariat to adopt the requirements of this Standard.

3. Context

3.1 Security screening is at the core of the *Policy on Government Security* as a fundamental practice that establishes and maintains a foundation of trust within government, between government and Canadians, and between Canada and other countries.

3.2 Security screening involves the collection of personal information from individuals, with their informed consent, and information from law enforcement and intelligence sources and other sources and methods to assess an individual's reliability and loyalty to Canada.

3.3 Security screening is conducted according to a common standard for most duties or positions in the federal government and for other individuals external to government with whom there is a need to share sensitive or classified information. Enhanced security screening may be conducted when duties involve or directly support security and intelligence functions, or involve access to security and intelligence sources and methodologies.

3.4 There are three different levels of security screening (see Appendix B for details):

- 3.4.1 Screening for reliability status assesses individuals' honesty and reliability.
- 3.4.2 Screening for a secret or top secret security clearance assesses individuals' loyalty to Canada and their reliability as it relates to that loyalty.

3.5 Another type of screening—site access screening—may be conducted for other individuals external to government who do not require access to sensitive information but who do require access to restricted or controlled government facilities or areas or within those facilities.

3.6 There are two types of site access screening (see Appendix B for details):

- 3.6.1 Screening for site access status assesses individuals' honesty and reliability.
- 3.6.2 Screening for site access clearance assesses individuals' loyalty to Canada and their reliability as it relates to that loyalty.

3.7 In all cases, individuals must be officially granted the required reliability status, secret security clearance, top secret security clearance, site access status or site access clearance (hereafter referred to as security status and/or security clearance) **before** they

are assigned duties or assigned to a position, and/or **before** they are granted access to sensitive information, assets or facilities. The decision by a deputy head or their delegate to grant a security status or clearance confirms that an individual is eligible to access sensitive information, assets or facilities.

3.8 Deputy heads have primary accountability for managing the security of their department or agency. In the context of security screening, this includes:

- 3.8.1 Determining their department or agency's specific security screening requirements;
- 3.8.2 Ensuring that all individuals who will have access to government information and assets, including those who work in or for offices of Ministers and Ministers of State, are security screened at the appropriate level before the commencement of their duties and are treated in a fair and unbiased manner; and
- 3.8.3 Ensuring that their authority to deny or revoke a security clearance is not delegated and, as appropriate, making or delegating authority to make all other security screening decisions.

3.9 To support deputy heads in exercising that accountability and in fulfilling policy requirements, this Standard defines the roles and responsibilities of executives and officials appointed to administer the delivery of security screening services, as well as those of employees in departments and agencies. It also establishes the Government of Canada's security screening model and practices to ensure that security screening is conducted effectively, rigorously and consistently.

3.10 This Standard encompasses a range of security practices that are to be implemented throughout an individual's engagement (i.e., employment, contract, appointment or assignment) with the Government of Canada, from initial screening through to aftercare, and reflects obligations pertaining to human resources management as well as legal and privacy imperatives, which are integral to the security screening process.

3.11 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.

3.12 Access to sensitive information, assets or facilities is a privilege, not a right. When individuals are granted a security status or clearance, they accept the responsibility for using, handling and protecting sensitive information, assets or facilities that accompany this privilege. They should not expect to have access to sensitive information, assets or facilities solely on the basis of their security status or clearance. Access is determined and provided on a need-to-know basis and can vary even among individuals who work in the same program area or who perform the same duties.

3.13 This Standard is issued pursuant to section 7 of the *Financial Administration Act*.

3.14 Treasury Board has delegated to the President of the Treasury Board the authority to issue and amend this Standard.

3.15 Department or agency requests for variations to the security screening model and criteria in Appendix B require the approval of the President of the Treasury Board. Any such requests require prior consultation with the Government Security Policy Division of Treasury Board of Canada Secretariat.

3.16 This Standard is to be read in conjunction with the *Foundation Framework for Treasury Board Policies*, the *Policy on Government Security*, the *Directive on Departmental Security Management*, the *Directive on Identity Management*, the *Security and Contracting Management Standard*, the *Policy on Privacy Protection* and the *Directive on Privacy Practices*.

4. Definitions

4.1 Definitions to be used in the interpretation of this Standard are in Appendix A and in the *Policy on Government Security*.

5. Statement

Objectives

5.1 The objectives of this Standard are to:

- 5.1.1 Ensure that security screening in the Government of Canada is effective, efficient, rigorous, consistent and fair; and
- 5.1.2 Enable greater transferability of security screening between departments and agencies.

Expected Results

5.2 The expected results of this Standard are:

- 5.2.1 Security screening services are effective and efficient, and meet the needs of departments and agencies, and of the Government of Canada as a whole;
- 5.2.2 Security screening practices provide reasonable assurance that individuals can be trusted to safeguard government information, assets and facilities, and to reliably fulfil their duties;
- 5.2.3 The collection, use, disclosure, retention and disposal of personal information for the purpose of security screening is done in accordance with the *Privacy Act* and other applicable legislation, policies and directives;
- 5.2.4 Individuals have an opportunity to explain adverse information before a decision is reached; and

- 5.2.5 Individuals are informed of their security responsibilities and of the consequences of not fulfilling them, and they apply them in accordance with the security status or clearance they have been granted.

6. Requirements

6.1 Executives and/or officials of organizations that are authorized to provide security screening services to departments and agencies are responsible for:

- 6.1.1 Establishing and overseeing the implementation and periodic review of the security screening procedures and practices described in the appendices to this Standard and, when appropriate, implementing measures to achieve process efficiencies in accordance with relevant legislation and policies;
- 6.1.2 Developing, in consultation with client departments and agencies, meaningful service standards to effectively manage performance, clarify clients expectations and drive service improvement, and mechanisms to ensure timely resolution of client service issues;
- 6.1.3 Maintaining appropriate security files for all individuals for whom security screening is conducted and ensuring that personal information for the purpose of security screening is collected, used, disclosed, retained and disposed of in accordance with the description, purpose, consistent use, and retention and disposal standards in the relevant personal information banks, and in compliance with applicable legislation;
- 6.1.4 Ensuring that relevant results of security screening are made available, upon request and in a timely manner, to the departmental security officer (DSO) or delegated official of a client department or agency and providing advice and recommendations to support decision-making;
- 6.1.5 Ensuring that persons or organizations that are assigned responsibility for conducting security screening are qualified to do so and that they perform their responsibilities in accordance with legal, ethical and policy requirements, and with the security interests of Canada;
- 6.1.6 Monitoring to ensure that the security screening services meet established service standards and that any issues relating to the fulfilment of service standards are investigated, acted on, and reported in a timely manner to, and in coordination with, the affected departments and agencies, and that they are shared with the Treasury Board of Canada Secretariat; and
- 6.1.7 Addressing issues of non-compliance with the requirements of this Standard in their department or agency.

6.2 Departmental security officers (DSOs) or delegated officials are responsible for:

- 6.2.1 Determining departmental or agency security screening requirements in accordance with the criteria established in Appendix B, identifying security screening decisions for which authority should be delegated, and obtaining deputy head approval of these requirements and delegations;
- 6.2.2 Establishing and overseeing the implementation and periodic review of security screening procedures and practices described in the appendices to this Standard, and, when appropriate, ensuring coordination with department or agency human resources management practices, including the following:
    - 6.2.2.1. Security screening activities;
    - 6.2.2.2. Collection, use, disclosure, retention and disposition of personal information for security screening;
    - 6.2.2.3. Evaluation, decision making, and review for cause;
    - 6.2.2.4. Review and rights of redress; and
    - 6.2.2.5. Aftercare;
- 6.2.3 Using security screening services where mandated or available to meet the departmental or agency security screening requirements, and verifying that the services obtained meet those requirements;
- 6.2.4 Ensuring that the security screening requirements of department or agency positions are reviewed periodically or when new programs or activities are established or substantially modified, and informing security screening service providers of any changes in requirements;
- 6.2.5 Ensuring that security screening requirements of departmental or agency positions that involve the provision of services to client departments or agencies are determined in consultation with the DSO or delegated official of the client department or agency;
- 6.2.6 Ensuring that, when adverse information is uncovered during the security screening process regarding an individual occupying a position that involves the provision of services to client departments or agencies, the DSO or delegated official and, as appropriate, the deputy head, of the client department is consulted before making a final decision to grant, grant with a waiver, deny or revoke a security status or clearance;
- 6.2.7 Acting as the sponsor when there is a requirement to conduct security screening of individuals external to government with whom the department or agency has a need to share sensitive information, and ensuring that the required status or clearance is granted before that information is shared;
- 6.2.8 Maintaining a security file for all individuals for whom security screening is conducted and ensuring that personal information for the purpose of security screening is collected, used, disclosed, retained and disposed of in accordance with the description, purpose, consistent use, and retention and disposal standards defined in the Standard Personal Information Bank – Personnel Security Screening;
- 6.2.9 Taking measures to address any actual or perceived security risk that presents or that may present a serious and immediate threat to the security of persons, the department or agency, or the government as a whole and, when appropriate, reporting such incidents to law enforcement authorities (e.g., police of jurisdiction), suspending an individual's security status or clearance pending an investigation, and consulting with human resources management regarding the suspension of an employee, as appropriate;
- 6.2.10 Ensuring that it is the deputy head who makes any decision to deny or revoke a security clearance and that individuals have an opportunity to explain adverse information before a decision is reached;

- 6.2.11 Reporting to the Canadian Security Intelligence Service any decision relating to an individual's security clearance, and any adverse information that could reasonably suggest that the individual may pose a threat to the security of Canada;
- 6.2.12 Consulting with the Treasury Board of Canada Secretariat on any proposed variation in the application of the security screening model, activities or practices outlined in Appendix B, and developing a business case, for the approval of the deputy head, to seek the approval of the President of the Treasury Board before implementing any changes; and
- 6.2.13 Addressing issues of non-compliance with the requirements of this Standard in their department or agency.

6.3 Managers are responsible for:

- 6.3.1 Ensuring that the requirement for a security status or clearance is established as a condition of employment, appointment, contract or other arrangement or assignment for which they are managerially responsible, and that this requirement is identified in relevant documentation (e.g., letters of offer, contracts, information-sharing agreements);
- 6.3.2 Ensuring that individuals for whom they are managerially responsible have a valid security status or clearance, as defined by the department or agency's security screening requirements, before:
    - 6.3.2.1. Issuing an unconditional job offer,
    - 6.3.2.2. Awarding a contract,
    - 6.3.2.3. Placing them in a position by means of other mechanism such as an assignment, secondment or volunteer, or
    - 6.3.2.4. Giving them access to sensitive government information and/or assets, or facilities; and
- 6.3.3 Monitoring for significant changes in behaviour of individuals for whom they are managerially responsible, and reporting these changes to the DSO or delegated official when there is reason to believe that such changes may pose a risk to departmental or agency or government security, and/or be cause for reviewing an individual's security status or clearance.

6.4 Individuals at all levels are responsible for:

- 6.4.1 Accurately and truthfully providing the personal information and evidentiary documents required for security screening, providing consent to conduct that screening, and doing so in accordance with the required format and established time frames and update cycles;
- 6.4.2 Notifying the DSO or delegated official of the following:
    - 6.4.2.1. Any change in personal circumstances that may affect the security status or clearance they have been granted;
    - 6.4.2.2. Any persistent or unusual contact, and of any attempt by another individual to solicit or obtain access to sensitive information, assets or facility without proper authorization; and
    - 6.4.2.3. Any unusual behaviour of individuals that may present a security risk to the department or agency or government as a whole, (as described in Appendix F); and
- 6.4.3 Performing their duties reliably and in compliance with the security status or clearance they are granted, the security obligations detailed on the security briefing form, and departmental security procedures.

7. Monitoring and reporting requirements

Within departments and agencies

7.1 Departmental security officers or delegated officials are responsible for:

- 7.1.1 Monitoring compliance with this Standard and the effectiveness of departmental or agency security procedures and practices.

By departments and agencies

7.2 Executives and/or officials of organizations that are authorized to provide security screening services to other departments and agencies are responsible for:

- 7.2.1 Reporting to the Treasury Board of Canada Secretariat the status and progress of implementing this Standard, and the results of ongoing performance measurement; and
- 7.2.2 Providing the Secretariat with relevant information to help inform government-wide policy direction and oversight.

7.3 Departmental security officers or delegated officials are responsible for:

- 7.3.1 Reporting to the Treasury Board of Canada Secretariat, upon request, the status and progress of implementing the departmental or agency requirements defined in this Standard, and the results of ongoing monitoring.

Government-wide

7.4 The Treasury Board of Canada Secretariat is responsible for:

- 7.4.1 Monitoring compliance with this Standard and the achievement of the expected results in a variety of ways, including the following:

        - 7.4.1.1. Management Accountability Framework assessments;
        - 7.4.1.2. The review of Treasury Board submissions, Departmental Performance Reports and Reports on Plans and Priorities;
        - 7.4.1.3. The review of Departmental Security Plans, progress reports and incident reports; and
        - 7.4.1.4. Results of performance measurement, program reviews, audits, evaluations and studies.
    - 7.4.2 Reviewing this Standard within five years of the effective date or more frequently, if required.

8. Consequences

8.1 Deputy heads, in consultation with the DSO or delegated official, are responsible for taking corrective measures in their department or agency to address issues of non-compliance with this Standard. Corrective measures can range from training, to the suspension or revocation of a security status or clearance, implementing requests from the Treasury Board of Canada Secretariat for corrective action, or any combination of these measures in keeping with the *Framework for the Management of Compliance*.

8.2 Departments and agencies are required to pay, from their budgets, any costs associated with inappropriate application of this Standard.

8.3 The consequences of non-compliance with this Standard are also described in Section 7 of the *Policy on Government Security*.

9. Roles and responsibilities of government departments and agencies

The following roles and responsibilities are supplementary to those defined in the *Policy on Government Security*.

9.1 The Treasury Board of Canada Secretariat is responsible for:

- 9.1.1 Issuing policy direction, guidance, tools and forms to support the implementation of this Standard;
- 9.1.2 Determining the personal information that is to be collected, used, disclosed, retained and disposed of for the purpose of security screening and maintaining the description of the Standard Personal Information Bank – Personnel Security Screening for this purpose;
- 9.1.3 Providing advice and guidance to departments and agencies on the implementation and interpretation of this Standard; and
- 9.1.4 Monitoring compliance with this Standard and the achievement of the expected results.

9.2 The Canadian Security Intelligence Service is responsible for:

- 9.2.1 Conducting, on behalf of departments and agencies, appraisals of individuals' loyalty to Canada and, so far as it relates thereto, their reliability; and
- 9.2.2 Maintaining an index of security assessments and a national registry of information and documentation that it receives on all persons who are designated as permanently bound to secrecy, as defined in the *Security of Information Act*.

9.3 Communications Security Establishment Canada is responsible for:

- 9.3.1 Defining criteria and formal control systems for access to Signals Intelligence (SIGINT) compartmented information, authorizing government departments to perform indoctrinations, and maintaining the national inventory of indoctrinated personnel.

9.4 Foreign Affairs, Trade and Development Canada is responsible for:

- 9.4.1 Conducting security screening of locally engaged staff and of other governments' officials at Canadian missions abroad.

9.5 The Department of National Defence is responsible for:

- 9.5.1 Processing requests for visits when security-cleared military personnel must visit a government or military establishment in Canada or abroad; and
- 9.5.2 Defining criteria and formal control systems for access to Talent-Keyhole compartmented information, authorizing government departments to perform indoctrinations, and maintaining the national inventory of indoctrinated personnel.

9.6 The Privy Council Office (PCO) is responsible for:

- 9.6.1 Providing advice to deputy heads who disagree with recommendations of the Security Intelligence Review Committee (SIRC) to grant or reinstate an individual's security clearance and ensuring that SIRC is informed in writing of the deputy head's final decision.

9.7 Public Works and Government Services Canada is responsible for:

- 9.7.1 Conducting security screening of private sector individuals as part of the government contracting process, including those participating in foreign contracts;

- 9.7.2 Managing a Visit Clearance Request system for visitors accessing classified information in private sector premises and for foreign private sector individuals accessing classified information in government premises.

9.8 The Royal Canadian Mounted Police is responsible for:

- 9.8.1 Maintaining a national repository of criminal history records to allow for criminal record checks to be conducted; and
- 9.8.2 Conducting law enforcement inquiries to verify whether an individual has been convicted of a criminal offence and, when appropriate, to assess the person's involvement with criminal organizations or with criminality, and potential vulnerabilities based on high-risk behaviours.

10. References

Legislation, Treasury Board policies, directives and standards, and Treasury Board Secretariat guidelines relevant to this Standard are listed in the *Policy on Government Security* and include the following:

- *Access to Information Act*
- *Canadian Charter of Rights and Freedoms*
- *Canadian Human Rights Act*
- *Canadian Security Intelligence Service Act*
- *Common ServicesPolicy*
- *Criminal Code*
- *Criminal Records Act*
- *Directive on Identity Management*
- *Directive on Privacy Practices*
- *Directive on Privacy Impact Assessments*
- *Directive on Privacy Requests and Correction of Personal Information*
- *Financial Administration Act*
- *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*
- *Guideline on Identity Assurance*
- *Guideline on Service Agreements: An Overview*
- *Guideline on Service Standards*
- *Guidelines for Discipline*
- *Guidelines for Termination or Demotion for Unsatisfactory Performance; Termination or Demotion for Reasons Other than Breaches of Discipline or Misconduct; and Termination of Employment During Probation*
- *Inquiries Act*
- *Policies for Ministers Offices*
- *Policy Framework for People Management*
- *Policy on Privacy Protection*
- *Privacy Act*
- *Public Service Labour Relations Act*
- *Security of Information Act*
- *Standard on Security in Contracting*
- *Youth Criminal Justice Act*

11. Enquiries

Please direct enquiries about this Standard to your departmental security officer (DSO) or delegated official. For interpretation of this Standard, the DSO or delegated official, or the executives appointed to administer the delivery of security screening services to departments and agencies should contact the Security and Identity Management Division.

Appendix A – Definitions

associations (*associations*)
: To unite with a connection or cooperative link with another or others in act, enterprise, business, partnership or collegially, in mind, imagination or person, as a partner, ally, or friend, and including but not limited to circumstances of accompaniment, attendance or presence at an event or with an entity.

administrative cancellation (*annulation pour des raisons administratives*)
: A decision recorded on an individual's security screening file that the security screening process has been discontinued and that is not recorded as a denial or revocation.

authoritative source (*source autorisée*)
: A collection or registry of records maintained by an authority that meets established criteria. (Source: *Standard on Identity and Credential Assurance*)

compartmented information (*information cloisonnée*)
: Information derived from sensitive sources and methods. Access to compartmented information is limited to Top Secret cleared Canadian citizens who are authorized to access the information after receiving a formal indoctrination. Compartments are implemented by controlling access to information using frameworks know as control systems. Control systems define who may

access the information, and under what conditions.

criminal conviction (*condamnation au criminel*)

The outcome of a criminal prosecution which concludes that an individual is guilty of an offence and has:

a. been convicted in Canada of an offence under an Act of Parliament punishable by way of an indictable offence or summary conviction, or
b. been convicted of an offence outside Canada that, if committed in Canada, would constitute an offence punishable by way of an indictable offence or summary conviction under an Act of Parliament.

criminal organization (*organisation criminelle*)

A group, however organized, that:

a. Is composed of three or more persons in or outside of Canada; and
b. Has, as one of its main purposes or main activities, the facilitation or commission of one or more serious offences that, if committed, would likely result in the direct or indirect receipt of a material benefit, including a financial benefit, by the group or by any of the persons who constitute the group.

It does not include a group of persons that forms randomly for the immediate commission of a single offence.
(Source: *Criminal Code*, section 467.1)

criminal record (*casier judiciaire*)

A record of criminal convictions and their dispositions, discharges, and outstanding entries including:

a. Criminal convictions contained in the Identification Databank of the Canadian Police Information Centre, RCMP National Repository of Criminal Records and/or police of jurisdiction databases; or
b. Foreign criminal convictions for offences which would have been an offence punishable by way of an indictable offence or summary conviction under Canadian law had it been committed in Canadian jurisdiction; or
c. Outstanding entries, such as charges, warrants, judicial orders, peace bonds, probation and prohibition orders; or
d. Absolute and conditional discharges as set out in section 730 of the *Criminal Code*.

Note: The release of criminal record information is governed by sections 4 to 6.4 of the *Criminal Records Act*, the *Youth Criminal Justice Act*, the *Privacy Act*, the *Criminal Code*, and directives from the Minister of Public Safety on the release of criminal record information.

enhanced screening (*filtrage approfondi)*

A type of security screening activity conducted when duties and access to information, assets or facilities are related to or directly support security and intelligence functions.

evidence of identity (*preuve de l'identité*)

A record from an authoritative source indicating an individual's identity. There are two categories of evidence of identity: foundational and supporting.

(Source:*Standard on Identity and Credential Assurance*)

foundational evidence of identity (*preuve de l'identité essentielle*)

Evidence of identity that establishes core identity information such as given name(s), surname, date of birth, sex and place of birth. Examples include records of birth, immigration or citizenship from an authority with the necessary jurisdiction.

(Source:*Standard on Identity and Credential Assurance*)

law enforcement inquiry (*enquête sur l'exécution de la loi*)

An examination of law enforcement authority records, databases or databanks to determine whether an individual:

a. Has a criminal record; and/or
b. Is associated with a criminal organization or known criminals; and/or
c. Is a dangerous offender; and/or
d. Is known, suspected of, or has engaged in criminality.

law enforcement authority (*organisme chargé de l'exécution de la loi*)

A body sanctioned by a municipal, provincial or national government to enforce laws and apprehend those who break them.

loyalty to Canada (*loyauté envers le Canada*)

A determination that an individual has not engaged, is not engaged, nor is likely to engage in activities that constitute a "threat to the security of Canada" as defined in section 2 of the *Canadian Security Intelligence Service Act*.

need to know (*besoin de savoir*)

A criterion used by the custodian(s) of sensitive information, assets or facilities to establish, prior to disclosure or providing access, that the intended recipient must have access to perform his or her official duties.

other individuals (*autres particuliers*)

Persons to whom government may need to provide access to sensitive information or assets, or access to facilities, through a formal arrangement that may include, but is not be limited to the following:

a. assignments (e.g., Interchange Canada assignments, detachment personnel);
b. contracts;

c. locally engaged staff at Canadian missions abroad;
d. domestic or international information-sharing agreements;
e. participation in special events (e.g., census);
f. volunteers (e.g., victim services / community policing volunteers);
g. federal/provincial/territorial (FPT) agreements ; or
h. critical infrastructure partnerships.

polygraph examination (*test polygraphique*)
An examination that uses questioning techniques and technology to record physiological responses which might indicate deception by an individual.

protected or restricted area or facility(*secteur ou installation à accès protégé ou restreint*)
An area or facility that is surrounded by a barrier or zoned as Operations, Security and High Security, where access is limited to individuals who have a valid security screening status or clearance.

qualified (*qualifié*)
Officially recognized as being trained, experienced and/or holding appropriate professional designation to perform a particular job.

reasonable assurance (*assurance raisonnable*)
A high degree of confidence that internal controls achieve intended objectives recognizing that external factors and inherent risk can impact and thereby limit the ability to provide absolute assurance of an individual's reliability or loyalty.

reliability status (*cote de fiabilité*)
The minimum standard of security screening for positions requiring unsupervised access to Government of Canada protected information, assets, facilities or information technology systems. Security screening for reliability status appraises an individual's honesty and whether he or she can be trusted to protect the employer's interests. Security screening for reliability status can include enhanced inquiries, verifications and assessments when duties involve or directly support security and intelligence functions. Reliability status may also be referred to herein as a security status.

security and intelligence functions (*activités de sécurité et de renseignement de sécurité*)
Functions that contribute to the safety of Canadians and the national security of Canada. These activities include efforts to detect, investigate and collect intelligence regarding threats posed by criminal organizations, malicious cyber actors, hostile intelligence organizations, foreign interference in Canadian affairs, or individuals engaged in criminality, espionage, terrorism or proliferation of weapons of mass destruction, and taking appropriate measures to prevent and protect against these threats while enforcing Canadian statues and supporting Canada's national interests.

security assessment (*évaluation de sécurité*)
An appraisal of an individual's loyalty to Canada and, so far as it relates thereto, the reliability of an individual. (Source: *Canadian Security Intelligence Service Act*, section 2)

security clearance (*autorisation de sécurité*)
The standard of security screening for all positions requiring access to Government of Canada classified information, assets, facilities or information technology systems. Security screening for a security clearance appraises an individual's loyalty to Canada and their reliability as it relates to that loyalty. Security screening for security clearance can include enhanced inquiries, verifications and assessments when duties involve or directly support security and intelligence functions.

security screening (*filtrage de sécurité*)
The process of conducting a security screening activity and evaluating an individual's reliability and/or loyalty to Canada in support of a decision to grant, grant with a waiver, deny, or revoke a reliability status, security clearance or site access clearance.

security waiver (*dispense de sécurité*)
A condition attached to the granting of a security status or clearance that details restrictions related to an individual's eligibility to access to sensitive information or assets, and facilities. A security waiver may be used when, despite concerns encountered in the security screening of an individual, a risk management decision is made to engage the individual on the basis that the duties cannot be performed by another.

sensitive information (*information délicate*)
Information categorized as protected (Protected A, Protected B or Protected C), classified (Confidential, Secret, Top Secret) or compartmented (Signals Intelligence, Talent Keyhole).

site access clearance (*autorisation d'accès aux sites*)
The standard of security screening for other individuals who are not employees, when duties do not require access to information but do require access to protected or restricted areas or facilities. Site access clearance is conducted when loyalty to Canada is the primary concern.

site access status (*cote d'accès aux sites*)
The standard of security screening conducted for other individuals who are not employees, when duties do not require access to information but do require access to protected or restricted areas or facilities. Site access status is conducted when reliability is the primary concern.

special access (*accès spécial*)
Compartmented information which is derived from sensitive sources, such as SIGINT or Talent Keyhole, in accordance with international bilateral agreements, which requires, as a prerequisite, Canadian citizenship and a Top Secret security clearance, and which is authorized through a formal indoctrination process.

sponsor (*parrain*)
One who conducts and/or arranges for the security screening of individuals with whom there is a need to share sensitive information which the Government of Canada is taking measures to protect, and who vouches for the security status or clearance of those individuals to other departments or agencies which may have a need to share sensitive information with the same individuals.

standard screening (*filtrage ordinaire*)
A type of security screening activity conducted when duties and access to information, assets or facilities are not related to and

do not directly support security and intelligence functions. Standard screening applies to most duties or positions and other individuals with whom there is a need to share sensitive information.

supporting evidence of identity(*preuve à l'appui de l'identité*)
Evidence of identity that corroborates the foundational evidence of identity and assists in linking the identity information to an individual. It may also provide additional information such as a photo, signature or address. Examples include social insurance records; records of entitlement to travel, drive or obtain health insurance; and records of marriage, death or name change originating from a jurisdictional authority. (Source:*Standard on Identity and Credential Assurance*)

threats to the security of Canada (*menaces envers la sécurité du Canada*)

a. espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
b. foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
c. activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and
d. activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*).
(Source: *Canadian Security Intelligence Act*)

vulnerable person (*personne vulnérable*)
A person who, because of his or her age, a disability or other circumstances, whether temporary or permanent,

a. is in a position of dependency on others; or
b. is otherwise at a greater risk than the general population of being harmed by a person in a position of trust or authority towards them.

(Source: *Criminal Records Act*)

vulnerable sector check (*vérification des antécédents en vue d'un travail auprès de personnes vulnérables*)
Pursuant to the *Criminal Records Act*, an examination of law enforcement authority records, including record suspensions for sex offences, databases, or databanks to assist departments and agencies in assessing the suitability of individuals in positions of trust or authority over vulnerable persons including children, the elderly and persons with disabilities. A vulnerable sector check involves the query of the following:

a. The Royal Canadian Mounted Police's National Repository of Criminal Records, including pardoned criminal files associated with sexually based criminal offences;
b. Canadian Police Information Centre Intelligence and investigative databanks; and
c. Police services records management systems where the applicant has resided.

Note: Information in relation to record suspensions obtained as a result of conducting a vulnerable sector check can only be used to screen individuals for positions of trust or authority over vulnerable persons.

Appendix B – Security Screening Model and Criteria

1. Security Screening Model

Security screening requirements are determined by the duties to be performed and by the sensitivity of information, assets or facilities to be accessed, and in accordance with the Position Analysis tool and guidance issued by the Secretariat.

Standard screening is conducted for all duties or positions in the federal government and for other individuals with whom there is a need to share or provide access to sensitive or classified information, assets or facilities, when responsibilities do not relate to security and intelligence functions.

Enhanced screening is conducted in limited and specific circumstances, and in accordance with the following criteria:

- When duties or positions involve, or directly support, security and intelligence (S&I) functions, including access to sensitive law enforcement or intelligence-related operational information, (i.e., sources or methodologies);
- When duties or positions involve direct joint operational activity with S&I departments or agencies;
- When duties or positions involve the provision of services to S&I departments or agencies which include management of, or access to, an aggregate of S&I information; or
- When duties or positions, and related access to sensitive information, create a high risk that an individual may be influenced by criminal or ideologically motivated persons or organizations.

There are three levels of security screening: reliability status, Secret security clearance, and Top Secret security clearance. Whenever the terms "status" or "clearance" are used, they encompass both standard and enhanced screening, unless otherwise specified.

The following table describes the standard and enhanced security screening activities.

Reliability Status	Secret Clearance	Top Secret Clearance

5 year background information

- Verification of identity and background
- Verification of educational and professional credentials
- Personal and professional references
- Financial inquiry (credit check)
- Law enforcement inquiry (criminal record check)

10 year background information

- Reliability status
- CSIS security assessment

10 year background information + foreign travel, foreign assets, character references, education, military service

- Reliability status / Secret clearance
- CSIS security assessment

Enhanced

- Law enforcement inquiry (Law enforcement record check (LERC))
- Security questionnaire and/or security interview
- Open source inquiry

Enhanced

- Security questionnaire and/or security interview
- Open source inquiry
- CSIS security assessment
- Polygraph examination

Validity Period	**Validity Period**	**Validity Period**
10 years	10 years	5 years

2. Criteria for Determining Level of Security Screening and Access Permissions

The criteria for determining the security screening requirements of positions are established in accordance with guidance issued by the Treasury Board of Canada Secretariat. Security screening requirements are based on criteria that reflect the following:

a. The duties to be performed;
b. The sensitivity of the information, assets or facilities to be accessed;
c. The level of authority or control exercised by the position; and
d. The degree of injury that could result from compromise of sensitive government information, assets or facilities to be accessed.

The following tables summarize how these criteria apply to each security status or clearance level and list the associated access permissions that may be granted.

In all cases, access to information, assets, facilities or information technology (IT) systems is determined and provided based on a need-to-know or need-to-access. Knowledge and access can vary even among individuals who work in the same department or program area or who perform the same duties.

Criteria for Determining Standard Screening

Standard ScreeningCriteria	**Access Permissions**
Reliability Status	
• Standard reliability status screening is the basic screening positions when duties require access to government information and assets, and unescorted access to operations zones in government facilities. • Standard reliability status screening must be conducted for all individuals employed by, or working in departments as defined in section 2 and any other agency included in Schedules IV and V of the *Financial Administration Act* (FAA), unless excluded by specific acts, regulations or orders-in-council. These include employees, volunteers, students or persons on loan, assignment or secondment, private sector contractors, and foreign and domestic visitors. • Its consistent and rigorous application underpins all subsequent levels of screening.	• Access to information, IT systems, and assets categorized as Protected A or B • Unescorted access to reception and operations zones of federal government facilities
Secret Clearance	

- Secret clearance screening builds on reliability status screening and is conducted for positions requiring frequent and unsupervised access to Government of Canada information, assets, facilities or IT systems categorized as secret
- It may also be required when duties:
- Could provide sufficient knowledge to obtain a comprehensive picture of a secret plan, policy or project;
- Require an individual to have access to certain levels of protectively marked material originating from another country or international organization;
- Require an individual to have access to systems deemed critical to the national interest that do not necessarily involve access to classified information or assets but that could cause major disruptions to the delivery of services to Canadians if compromised; or
- Involve working in offices of or for ministers, ministers of state and parliamentary secretaries, including exempt staff.

- Regular access to information, IT systems, and assets categorized as Protected A or B , Confidential and Secret
- Unescorted access to reception, operations, and security zones of certain federal government facilities
- Access to systems in security zones with permissions such as may be required for the purpose of maintenance, monitoring, detection, back-up and recovery, testing, installation and configuration changes

Top Secret Clearance

- Top Secret clearance screening is conducted for positions requiring frequent and unsupervised access to top secret Government of Canada information, assets, facilities or IT systems.
- It may also be required when duties:
- Provide sufficient knowledge to obtain a comprehensive picture of a top secret Government of Canada plan, policy or project;
- Require an individual to have access to certain levels of protectively marked material originating from another country or international organization; or
- Require an individual to have access to classified information, assets or facilities where the impact of wrongdoing would cause extremely serious injury to the national interest and pose a threat to the security of Canada.
- A Top Secret clearance is a prerequisite for access to some compartmented information.

- Access to information, IT systems, and assets categorized as Protected A or B , orClassifiedat any level
- Unescorted access to reception, operations, and security and high-security zones of certain federal government facilities
- Restricted access to specific top secret networks or systems in high-security zones

Criteria for Determining Enhanced Screening

Enhanced Screening Criteria	Access Permissions
Reliability Status	
• Enhanced reliability status screening is the basic screening for positions that perform security and intelligence functions or duties that support those functions. • It is required for positions requiring long-term, frequent and uncontrolled access to law enforcement or criminal intelligence information, assets or facilities and involves a more thorough examination of an individual's reliability. • It may also be conducted for positions when duties support security and intelligence functions or operations. • Its consistent and rigorous application underpins all subsequent enhanced screening.	• Access to information, IT systems, and assets categorized as Protected A, B or C • Access to certain levels of protectively marked material originating from other countries or international organization • Unescorted access to reception and operations zones of federal government law enforcement and some security and intelligence facilities, and other federal government facilities
Secret Clearance	
• A Secret security clearance conducted for positions that perform security and intelligence functions, or duties that support those functions and that require long-term, frequent and unsupervised access to secret law enforcement information, assets, facilities or IT systems.	• Regular access to information, IT systems, and assets categorized as Protected A, B, C, Confidential and Secret • Unescorted access to reception, operations, and some security zones of federal government law enforcement facilities, and other federal government facilities • Access to information technology systems in some security zones with permissions such as may be required for the purpose of maintenance, monitoring, detection, back-up

and recovery, testing, installation and configuration changes

Top Secret Clearance

- Enhanced screening is conducted for certain positions in the security and intelligence community that require regular and unsupervised access to methods, sources, analytical processes and techniques related to the collection of sensitive or classified intelligence or counter-intelligence information.
- It is also required for positions that require long-term, frequent and uncontrolled access to top secret assets or facilities
- An enhanced Top Secret clearance can be a prerequisite for access to some compartmented information where the nature of the collection technique used in obtaining that information is evident.

- Access to government information, IT systems, and assets categorized as Protected or Classified at any level
- Unescorted access to reception, operations, and security and high-security zones federal government law enforcement and security and intelligence facilities, and other federal government facilities
- Access to specific top secret networks or systems in high-security zones

3. Access to Compartmented Information

A security clearance alone does not permit access to compartmented information. Access to compartmented information requires authorization in accordance with the standards set by the control system owner for each control system to which access is required. These standards include a briefing and signed acknowledgement by the individual of their responsibility to protect compartmented information from unauthorized exposure. Once an individual is given access they must handle the compartmented information according to the standards set by the control system owner.

4. Site Access Screening

Site Access screening is conducted when there is a need for other individuals, who are not employees, to have access to restricted or protected areas or facilities. Site Access screening does not provide for access to sensitive government information.

Security screening for site access must be demonstrably proportionate to the perceived risk and appropriate to the situation. In some circumstances, it may be a preferable option to escort workers rather than to conduct security screening when the risk is low or access is required on a "one-off" basis. On the other hand, security screening in itself may not necessarily eliminate the need to escort workers when the possibility to cause injury is high.

There are two types of site access screening: site access status and site access clearance. Site access status is conducted when **reliability** is the primary concern. Site access clearance may be conducted when **loyalty to Canada** is the primary concern.

Site Access Status

5 year background information

- Verification of identity
- Law enforcement inquiry (criminal record check)

Site Access Clearance

5 year background information

- Verification of identity
- Law enforcement inquiry (criminal record check)
- Security Assessment (CSIS)

Additional inquiries, verifications or assessments may be conducted as defined by the Position Analysis Tool and can include: personal and professional references, security interview, law enforcement record check (LERC), and/or polygraph examination.

Validity period
Up to 10 years.
Security screening may be updated more frequently when employment has lapsed for 12 months or more.

Criteria for Determining Type of Site Access Screening

The criteria for determining the type of site access screening is established in accordance with guidance issued by the

Treasury Board of Canada Secretariat. Security screening requirements are based on criteria that reflect the following:

a. The nature of department or program operations;
b. Whether the individual will be escorted or unescorted;
c. Whether the individual requires access to the exterior or interior of a facility;
d. Whether the primary security concerns relate to reliability or loyalty; and
e. The possibility of the individual overviewing or overhearing sensitive conversations.

5. Update Requirements for Reliability Status, Secret, and Top Secret Clearances

The following table identifies the screening activities and update cycles for each type of security screening. In general, security screening activities conducted for initial screening should not be redone unless they were not done or were improperly done originally.

Security Screening Updates	Update Cycle
Reliability Status	
• Updated application form covering period since last update • Financial inquiry • Law enforcement inquiry	10 years
Enhanced (also includes) • Security questionnaire and/or security interview • Open-source inquiry	
Secret Clearance	
• Updated application form covering period since last update • Valid standard reliability status • CSIS security assessment	10 years
Top Secret Clearance	
• Updated application form covering period since last update • Valid standard reliability status • CSIS security assessment	5 years
Enhanced (also includes) • Security questionnaire and/or security interview • Open-source inquiry • Polygraph examination	

6. Update Requirements for Site Access Screening

Site Access screening can be valid for up to ten years from the date of issue. However, since Site Access screening is conducted for other individuals who may not be engaged with the federal government on an on-going basis, practices related to reactivation and expiry described in Appendix F will apply in respect of security screening verifications, inquiries and assessment which may be repeated when the person has not been engaged or inactive for a period of 12 months or more. The following table identifies the screening activities and update cycles for site access screening and the associated security screening activities

Site Access Status

5 year background information

- Verification of identity
- Law enforcement inquiry (criminal record check)

Site Access Clearance

5 year background information

- Verification of identity
- Law enforcement inquiry (criminal record check)
- Security Assessment (CSIS)

Additional inquiries, verifications or assessments may be conducted as defined by the Position Analysis Tool and can include: personal and professional references, security interview, law enforcement record check (LERC), and/or polygraph examination.

Validity period
Up to 10 years.
Security screening may be updated more frequently when employment has lapsed for 12 months or more.

7. Security Screening Activities and Practices

The following table describes the purpose and practices associated with each security screening activity and how they serve to assess an individual's reliability or loyalty to Canada, as applicable.

The models in the preceding pages identify the security screening activities associated with each status or clearance for both initial screening and for updates. Certain security screening activities may also be conducted when the duties or position warrant additional security screening as defined by the Position Analysis Tool or for cause when information is uncovered or reported about an individual that may call into question his or her reliability or loyalty to Canada.

In general, security screening activities associated with reliability status are conducted in a particular order to ensure that the basic elements of honesty and trustworthiness are established before more in-depth verifications, inquiries or assessments are undertaken. Once basic reliability is substantiated, some security screening activities may be conducted in parallel.

Activity	Purpose	Practice
Identity and background verification	• Validate an individual's unique identity and biographical information • Ensure that all subsequent security screening activities are conducted in relation to the actual individual • Ensure that identity information uniquely distinguishes the individual, is confirmed as accurate, and relates to the individual making the claim.	• Evidence of identity is verified in accordance with the *Standard on Identity and Credential Assurance* and the *Guideline on Identity Assurance*. • Level 3 identity and credential assurance is the minimum level required for all types of security screening. • Accuracy of the individual's background is verified (e.g., residence, employment). • If an individual's personal history cannot be established for the period of time required by the type of screening (i.e., 5 or 10 years), information relating to the person's trustworthiness, including, where available, a criminal record check from each country in which the person has resided for one or more years in the last five years, may be required. **Note**: Identity must be verified before undertaking any subsequent security screening activity.
Educational and professional credential verification	• Assess an individual's honesty and trustworthiness	• Relevant educational and professional credentials and designations are verified. • An individual's past or current behaviour, ideologies or associations may also be inquired about.
Personal and professional reference checks	• Assess an individual's reliability and loyalty on the basis of statements obtained from people who know the individual	• Information about the individual is obtained from and/or validated with persons who know or who are in a position to observe the individual. • Inquiries may relate to the individual's character, associations, reliability, and loyalty in previous employment, and activities in or outside the workplace.
	• Determine whether an individual has a criminal record • Determine whether an individual has any outstanding warrants or	• Law enforcement inquiries include, as a minimum for all types of screening, verification of a criminal record against the Royal Canadian Mounted Police's (RCMP's) National Repository of Criminal Records. It may also include an inquiry of other national or local police databases. • Law enforcement inquiries may also include, for individuals undergoing enhanced screening, an examination of other RCMP and jurisdictional police agency records to verify the existence of outstanding warrants or prohibitions, or to assess whether an individual has any associations with or has engaged, is engaged,

Law enforcement inquiry	outstanding warrants or prohibitions • Assess whether an individual is known, suspected of, or associated with individuals or organizations that are known or suspected of engaging in or being associated with organized crime	may engage, or may be induced to engage in activities related to organized crime. • Vulnerable sector checks should be conducted when duties involve responsibility for the well-being of, or exercise of authority over, vulnerable persons (e.g., children, the elderly, and persons with disabilities). Positions subject to this type of inquiry may include but not be limited to prison guards or matrons, cadet instructors under the National Defence portfolio, volunteers, victim service workers, and health professionals. • Reports will not reveal operational methodologies or intelligence sources of the RCMP or police agency of jurisdiction. **Note**: A record of a conviction in respect of which a record suspension has been ordered shall not be disclosed, nor shall the existence of the record or the fact of the conviction be disclosed, without the prior approval of the Minister of Public Safety.
Financial inquiry	• Assess whether an individual poses a security risk on the basis of financial pressure or history of poor financial responsibility	• Financial inquiries include, as a minimum, a full consumer credit report from a credit reporting agency. The report provides information on the individual's credit history, liens, judgments and bankruptcy but does not include a credit score. • Credit checks conducted for the purpose of security screening are "masked" so that no adverse effect is brought to the individual's credit bureau file. • A financial assessment questionnaire may also be administered for individuals undergoing enhanced screening, in particular those performing S&I functions, to determine whether an individual may pose a security risk on the basis of financial obligations. • Alternate methods of conducting a financial inquiry may be established when legitimate credit reporting agencies are not available (e.g. for locally engaged staff at Canadian missions abroad).
CSIS security assessment	• Assess an individual's loyalty to Canada and so far as it relates thereto, the individual's reliability	• A security assessment involves verification of CSIS databases and other methods to assess whether there is reasonable cause to believe that an individual has engaged, is engaged, or may engage in activities that constitute a "threat to the security of Canada," as defined in section 2 of the *Canadian Security Intelligence Service Act*. • Any report will not reveal CSIS operational methodologies or intelligence sources. • A CSIS security assessment may be conducted in limited and specific circumstances for individuals who do not require access to classified information but do require access to restricted or controlled facilities (e.g., locally engaged staff at Canadian missions abroad).
Security questionnaire	• Assess an individual's reliability and/or loyalty to Canada	• The individual being screened completes a questionnaire to determine whether he or she may pose a security risk on the basis of ideology, conduct, associations, or features of character. • The questionnaire covers a range of topics related to personal activities, including finances, involvement with illegal drugs, alcohol use, associations, use of computers and technology, online presence, and loyalty to Canada.
Security interview	• Assess an individual's reliability and/or loyalty to Canada	• The individual being screened is interviewed to determine whether he or she may pose a security risk on the basis of ideology, conduct, associations, or features of character. • Security interviews are normally conducted in person but on rare occasions may be conducted by phone or by video conference. • In general, interview questions cover the time frame associated with the level of security screening. • The interviews are normally recorded using appropriate and available means (e.g., in writing, or in an audio or video recording), and only with the specific consent of the individual. • Security interviews may also be conducted when not otherwise indicated as a mandatory security screening activity when adverse information is uncovered, for cause, or for access to

		compartmented information.
Open-source inquiry	• Assess an individual's reliability and/or loyalty to Canada,	• Open-source information is analyzed to verify background information provided by the individual and to identify behaviour that may be inconsistent with security responsibilities. • Open-source information is handled in the same manner as any other information collected through the security screening process to ensure that an individual's privacy is respected and to ensure that the information is relevant, reliable and attributable. • Open-source information is publicly available and may include but is not limited to the following: • Internet: Web-based communities and user-generated content, social-networking sites, video-sharing sites, wikis, and blogs; • Media: Newspapers, magazines, radio, television and computer-based information; • Public data: Government reports, official data such as budgets, hearings, legislative debates, press conferences, speeches and contract awards; and • Professional and academic: Conferences, symposia, professional associations, academic papers and subject-matter experts. • Open source checks may be conducted when not otherwise indicated as a mandatory security screening activity when adverse information is uncovered, for cause, or for the purpose of periodic monitoring as part of Aftercare (maintenance).
Polygraph examination	• Assess an individual's criminality and/or loyalty to Canada	• Polygraph examinations use questioning techniques and technology to record physiological responses which might indicate deception by the individual. • Testing questions relate to relevant details of the individual's behaviour collected through other security verifications, inquiries or assessments. • Examinations are administered by qualified personnel according to recognized techniques and written standards that are designed to protect individuals' legal rights and rights under the *Canadian Charter of Rights and Freedoms*.

Appendix C – Collection, Use, Disclosure, Retention and Disposal of Personal Information for the Purpose of Security Screening

1. General

The collection, use, disclosure, retention and disposal of personal information for the purpose of security screening is carried out in accordance with the *Privacy Act* and associated policies, directives, standards and guidelines.

The description, purpose and consistent uses of that information are contained in the relevant Standard Personal Information Banks found in Info Source. Info Source provides information about the functions, programs, activities and related information holdings of government institutions subject to the *Access to Information Act* and the *Privacy Act*; and provides government employees (current and former) and other individuals with relevant information to help them access personal information about themselves held by government institutions subject to the *Privacy Act* and to exercise their rights under the *Privacy Act*.

2. Forms for the Collection of Personal Information

Personal information for the purpose of security screening is collected from individuals using forms and tools issued and/or approved by the Treasury Board of Canada Secretariat (TBS). Security screening forms are designed to collect relevant, verifiable information about an individual and, when appropriate to the type of screening, information about the individual's spouse, co-habitants and family members.

Individuals may also be required to provide other personal information to support the security screening process. That information may include vital events credentials (e.g., birth certificate, passport), biometrics (e.g., digital photographs, fingerprints), or letters of reference or referral (see the section titled "Out-of-Country Checks" in Appendix D).

3. Automated Security Screening Application Forms and Repositories

All forms produced to automate the collection, disclosure and handling of personal information for security screening must be designed to collect only the specific elements or categories of information required for the screening, as defined in the TBS-issued forms.

Requirements pertaining to the collection, use, disclosure, retention and disposal of information, as defined in Standard Personal Information Bank PSU 917 (Personnel Security Screening) apply equally to automated repositories, as do other procedures outlined in this Standard and in other Treasury Board policies, directives, standards and guidelines.

Before any system to collect, process and manage personal information is put into operation, a risk assessment and a privacy impact assessment must be conducted, and security and privacy concerns must be mitigated to ensure that personal information is protected in accordance with the *Privacy Act* and related policy instruments.

4. Personal Information Banks

Personal information created, collected, used, disclosed and retained for the purpose of security screening is defined in Standard Personal Information Bank PSU 917 (Personnel Security Screening).

Personal information of contractors collected, used, disclosed and retained for the purpose of security screening is defined in Public Works and Government Services Canada's PCU 015 (Industry Personnel Clearance and Reliability Records).

Departments and agencies that maintain institution-specific personal information banks must ensure that they are kept up to date to reflect, at a minimum, the purpose, uses, disclosure, retention and disposal of information defined in PSU 917 (Personnel Security Screening).

To facilitate cross-referencing, the following Standard Personal Information Banks are also authorized to contain a copy of the Security Screening Certificate and Briefing Form:

a. Employee Personnel Record (PSE 901);
b. Governor in Council Appointments (PSU 918);
c. Members of Boards, Committees and Councils (PSU 919);
d. Identification and Building-Pass Cards (PSE 917); and
e. Security Incidents (PSU 939).

5. Consent

In order for security screening to be conducted, individuals must provide their consent. By consenting, they authorize the indirect collection and the disclosure of information for security screening purposes. Until consent is obtained, information cannot be collected, used or disclosed.

Consent must be obtained for all initial security screenings, and it remains valid for updates or reviews of status or clearance for as long as an individual remains an employee or under contract or assignment to the Crown, or until the individual formally withdraws consent.

Although consent remains valid for the duration of employment, as a matter of prudence, individuals should be given the opportunity to confirm or withdraw their consent each time they complete forms for the purpose of security screening. If the security screening requirements have changed since the last time the individual's consent was obtained, consent must be confirmed to ensure that the person understands the security screening activities being consented to.

Only applicants who have reached the age of 18 can provide consent. When security screening is being conducted for an individual who has not yet reached the age of 18, the consent of a parent or guardian is required.

6. Non-Consent or Failure to Provide Information

When an individual persistently delays, refuses to provide, or withdraws, in full or in part, consent or willingness to provide supporting documentation (e.g., vital events credentials, biometrics) for an initial security screening, screening activities are to cease and the person is to be informed that:

a. Security screening cannot continue without his or her consent or the required documentation or information;
b. Failure to provide consent or the required documentation or information will result in his or her no longer being considered for appointment, employment, contract or assignment; and
c. The security screening action will be administratively cancelled until the required documentation or information is obtained. (**Note:** Administrative cancellation of security screening is not recorded as a denial or revocation of status or clearance.)

When an individual's security status or clearance is being updated or upgraded and the person refuses to provide consent or the required information, the person's existing security status or clearance must be suspended and reviewed for cause, and the human resources unit should be consulted.

Consequences to individuals for not providing consent or for failing to provide information can include administrative cancellation of their security status or clearance. This administrative cancellation will result in the individual no longer meeting the condition of employment and could result in termination of employment or cancellation of a contract.

7. Disclosure and Data Validation

Personal information collected in security screening forms must be disclosed to security screening service providers both in government (e.g., the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP)) and

outside government (e.g., credit bureaus) in order for the verifications, inquiries and assessments required for security screening to be conducted.

These verifications, inquiries and assessments can include the validation of personal information against operational records, data banks, data holdings, and intelligence sources for the purpose of assessing an individual's reliability and/or loyalty.

Personal information, combined with the decision to grant, grant with a security waiver, deny, revoke or suspend a security status or clearance, may also be used to create a security profile for the purpose of managing Government of Canada credentials required to access information, assets and facilities (e.g., building passes and digital certificates). The relevant personal information banks need to reflect the purposes, uses and disclosure of information and be kept up to date.

8. Protection of Personal Information

Personal information created, collected, used, disclosed, retained and disposed of for the purpose of security screening will be safeguarded in accordance with government standards for the protection of personal information, as well as the *Directive on Privacy Practices*. The level of categorization, and thereby protection, depends primarily on the sensitivity of the reports produced by CSIS or the RCMP.

Access to, disclosure and handling of personal security screening information is to be monitored, documented, and limited to those who have a need to access it and who have a valid security status or clearance, using appropriate administrative, technical and physical security controls.

9. Security Screening File Management

Files will be created for each individual who undergoes security screening. These files contain relevant personal information, actions taken and decisions rendered in relation to the individual's security screening. Security screening service providers may also maintain records for audit purposes and for use when conducting security screening for updates or upgrades.

Staff responsible for maintaining security screening files must take all reasonable steps to ensure that personal information is accurate, up-to-date and appropriately protected. Security screening files are to be updated whenever a change is reported in an individual's personal circumstances (e.g., a criminal conviction, personal bankruptcy), and whenever there is a change in an individual's security status or clearance (e.g., update, upgrade, administrative cancellation). Any decisions made with respect to these actions, as well as the rationale for the decisions, must be recorded. All information related to criminal offences for which the individual received a suspension must be removed from the file.

The following information is to be recorded, maintained and updated as necessary:

a. Completed original copies of security screening forms and questionnaires;
b. Relevant results of all security screening verifications, inquiries and assessments;
c. Analysis of results and any advice or recommendations to support decision-making;
d. Decisions to grant, grant with a security waiver, deny, revoke, suspend pending investigation, or administratively cancel a security status or clearance; and
e. Relevant information related to any waiver, temporary access, review for cause, or investigation, and any ensuing decisions.

10. File Exchange

When an individual changes department or agency, permanently or temporarily, or when a contractor moves between contracts, the individual's security file will be made available or transferred, in the case of a permanent move, to the receiving departmental security officer (DSO) or delegated official, upon request and in a timely manner. With the following exceptions, the contents of the file should not be removed or withheld from the receiving department:

a. When the file contains a classified CSIS security assessment, the sending department or agency must remove the assessment from file, return it to CSIS, and advise the DSO or delegated official of the receiving department of the existence of the assessment who will obtain an updated assessment from CSIS before rendering a decision; and
b. When the file contains a record of discharge under section 730 of the *Criminal Code*, it is not to be disclosed to any person or transferred to another department or agency, nor shall the existence of the record or the fact of the discharge be disclosed without prior approval of the Minister of Public Safety if:
    - More than one year has elapsed since the individual was discharged absolutely; or
    - More than three years have elapsed since the individual was discharged on the conditions prescribed in a probation order.

Any other adverse information must be revalidated with the appropriate security screening service provider before a decision is rendered to ensure that the information is still relevant. As appropriate, updated information required for the security status or clearance should be obtained and evaluated by the receiving department or agency before a decision is made to accept the transfer.

11. Department- or Agency-Specific Indices Checks

A few departments or agencies may have authority to conduct inquiries against data sources they maintain. For example, the Canada Revenue Agency (CRA), as a separate employer, may query its internal intelligence sources to assess an individual's suitability for employment with it. The results of these types of department-specific checks cannot be included in an individual's

security screening file or shared with another department, including security screening service providers.

12. File Retention and Disposition

Security screening files contained in Personal Information Bank PSU 917 (Personnel Security Screening) are retained for at least two years following an individual's departure from the federal public service to ensure that the individual has a reasonable opportunity to obtain access to the information in his or her file. CSIS may retain records of assessments and associated information relating to the file for longer because of Security Intelligence Review Committee requirements or because of national security requirements.

When a request for access to the information has been received, the information will not be destroyed until such time as the individual has had the opportunity to exercise all of his or her rights under the *Privacy Act* or the *Access to Information Act*.

Security screening files of individuals who have been denied or revoked a security status or clearance will be retained for at least 10 years following their departure from the federal public service before being destroyed to help ensure that these individuals are not engaged by a department or agency without regard to the denial or revocation.

Security screening files of individuals who have left the employment of the federal public service are not transferred to the departmental Personnel Records Centre or to any Federal Records Centre of Library and Archives Canada.

Appendix D – Evaluation, Decision Making, and Review for Cause

1. General

Decisions about an individual's security status or clearance are based on information gathered during the security screening process.

The information that is gathered is analyzed to ensure that it is pertinent to the decision being made, that it is derived from one or more authoritative sources that report the same facts, and that it is attributable to the individual who is being assessed.

Decision making involves evaluating the sensitivity of the position and the work environment in which the duties will be performed; evaluating the risks associated with making the appointment or issuing a contract, or with giving the individual access to sensitive information, assets, or facilities; and a judgment of whether such risks are acceptable. The decision must be based on an adequate amount of verifiable information to ensure that it is fair, objective and defensible. The final decision is the responsibility of the deputy head or delegated official.

A negative decision may be rendered when information is uncovered that raises a reasonable doubt as to an individual's reliability or loyalty to Canada. A negative decision means that an individual cannot be issued an unconditional offer of employment, appointed to a position, assigned duties, or awarded a contract. When consideration is being given to rendering a negative decision, individuals must be informed, provided with reasons for the decision (unless the information is not to be disclosed under the *Privacy Act* or other applicable legislation) and given an opportunity to respond to the information.

All information considered in rendering a decision, along with any follow-up action and the decision itself, must be recorded in the individual's security screening file. Decisions made to grant, deny, revoke, suspend or administratively cancel a clearance or a site access clearance must be communicated to the Canadian Security Intelligence Service (CSIS) so that it can update its systems accordingly.

2. Analysis and Evaluation

In arriving at a security screening decision, officials are expected to provide a fair and objective evaluation that respects the rights of the individual.

Adverse information concerning an individual is assessed with respect to the following:

- Its nature and seriousness;
- How recent it is;
- The surrounding circumstances, including frequency of the incident(s), the individual's willingness to participate, the individual's maturity at the time of the incident(s), the degree of rehabilitation since the incident(s), the potential for pressure, coercion, exploitation or duress; and
- Its implications for the individual's reliability and whether the individual has been open about the information and has resolved, or appears likely to resolve, the concerns to which it gives rise.

When considering the significance of personal circumstances or behaviour that could lead to vulnerability, officials will not allow their own personal and cultural bias to affect their judgment. An individual's personal circumstances or behaviour are only of security significance if they cause vulnerability to pressure or improper influence, or if they could cause the individual to commit a security breach.

Individuals will be notified when a security status or clearance has been granted.

When consideration is being given to denying or revoking a security status or clearance, individuals must be informed in writing and be provided with reasons, unless the information is not to be disclosed under the *Privacy Act* or other applicable legislation. They must also be given an opportunity to validate or refute adverse information.

The following sections summarize the most typical concerns encountered in security screening, matters to be taken into consideration when rendering a decision, and required action.

3. Unverifiable identity and biographical information

Normally, when identity or biographical information cannot be verified despite reasonable, genuine and demonstrable effort, a decision cannot be made and the security status or clearance must be denied and the individual advised of his or her rights of redress.

The verification of biographical information typically covers the number of years of background information required by the specific level of security status or clearance. The inability to verify the required number of years of background information, however, must not be considered as an absolute reason not to grant a security status or clearance. Efforts must be made to avoid systematically applying, or appearing to do so, the requirement for the specified number of years of background information. A degree of latitude should be provided when considering the period of coverage that can be obtained.

Before rendering a decision to deny a security status or clearance:

a. Reasonable and genuine efforts must be made to obtain the necessary information and be shown to have failed;
b. In the absence of some but not all of the required years of background information, efforts must be made to consider reasonable alternative forms of information about the individual from substitute sources, such as additional references, and/or a security interview to give the individual an opportunity to explain the circumstances and to correct or provide additional information; and
c. A determination must be made that such alternative measures cannot mitigate the risk associated with granting the individual the required security status or clearance.

4. Out-of-Country Checks

For security screening to be meaningful and accurate, individuals must have lived in Canada for a sufficient period of time to enable appropriate inquiries, verifications and assessments to be conducted. Although a lack of sufficient Canadian residency in and of itself is not necessarily a barrier to the granting of a security status or clearance, decision makers will need to consider what checks can be carried out and the information available upon which to make a decision. Depending on the status or clearance required, this may range from 5 to 10 years.

Individuals who have lived outside of Canada for longer than six months in a row within the time period required by the security status or clearance will be required to account for their activities during that time, unless the time spent abroad was related to their employment or assignment with a Government of Canada department or agency or with the Canadian Armed Forces. Such accounting could include the following:

a. Letters of reference or referral from foreign embassies and missions in Canada;
b. Canadian embassies or missions in the country in which the individual resided;
c. Information from counterpart security screening organizations in countries with which Canada has entered into bilateral arrangements for the exchange of security screening information;
d. Letters or police clearance certificates from law enforcement agencies in the country in which the individual resided; and
e. Credit summaries from established foreign financial institutions or letters of reference from foreign educational institutions or universities.

Activities accounted for in these ways will be assessed in consideration of the adequacy and reliability of the originating country's record-keeping systems.

Police clearance certificates are different in each country and may also be known by other names, including good conduct certificates and judicial record extracts. The certificates should provide a summary of an individual's criminal record or a declaration of the absence of any criminal record.

If an individual has resided, or currently resides, outside of Canada, information on how to obtain a police clearance certificate can be found on the Citizenship and Immigration Canada's web site.

If an individual has resided, or currently resides, in the United States, the individual may be required to obtain a police clearance certificate from the state police.

5. Criminal Record

The existence of a criminal record can, but may not be, sufficient grounds to deny or revoke a security status or clearance. A criminal record is to be considered in light of matters such as the type of criminal activity, the duties to be performed, the nature and frequency of the offence, and the passage of time.

All information relating to criminal record must be verified. For example, an individual might not report having one, but might have one; an individual might report having one, but the information reported about it might differ from the information reported by the RCMP. A criminal offence for which a suspension has been granted must not be inquired about.

An individual convicted of any of the offences listed in subsection 750(3) of the *Criminal Code* cannot be granted a security status or clearance unless an order of restoration is granted to that person by the Governor in Council.

6. Adverse Information

Adverse information can, but may not be, sufficient grounds to deny or revoke a security status or clearance. When uncovered, such information is to be used as the basis for further investigation, including a security interview.

When adverse information reflects a recent or recurring pattern of questionable judgment that may negatively affect the performance of duties or that may lead to an inability or unwillingness to safeguard sensitive information, assets or facilities, a review for cause of the security status or clearance previously granted to the individual must be conducted.

When adverse information is uncovered that provides reasonable grounds to suspect that the individual may pose a serious threat to others, or may be involved in fraud or other criminal conduct, the information may be disclosed to law enforcement authorities (e.g., police of jurisdiction).

7. Adverse Security Assessment

Adverse information obtained pursuant to a CSIS security assessment is the primary determinant of whether a security clearance or site access clearance can be granted. If there are reasonable grounds to believe that either of the following conditions applies, the security clearance or site access clearance may be denied, revoked, or suspended pending further investigation, as appropriate:

a) In the case of loyalty, the individual has engaged, is engaged, may engage, or may be induced to engage in activities that constitute a threat to the security of Canada as that term is defined in the *Canadian Security Intelligence Service Act*; or

b) In the case of reliability as it relates to loyalty, because of personal beliefs, features of character, association with persons or groups considered a security threat, or family or other close ties to persons living in countries that pose a security risk to Canada, the individual has acted, is acting, may act or may be induced to act in a way that constitutes a threat to the security of Canada; or the individual has disclosed, may disclose, may be induced to disclose, or may cause to be disclosed in an unauthorized way, sensitive information.

If adverse information is uncovered related to the reliability or loyalty of an individual who is undergoing or who has undergone security screening, it must be reported to the DSO or to the designated security official of client departments and agencies so that appropriate action can be taken to review for cause, deny, or revoke, as appropriate, a security clearance or site access clearance.

8. Security Interview to Resolve Doubt

A security interview, in addition to being a standard component of enhanced security screening, can also be used as a means to resolve doubt or to address adverse information that is uncovered during security screening. A security interview provides an opportunity for the screening official and the individual to discuss any matters of concern and gives the individual the opportunity to explain the situation before a decision is rendered.

Individuals are to be provided with a statement summarizing the information available to enable them to be reasonably informed of the adverse or missing information, without disclosing any information that could injure national security or endanger the safety of any person, or that would be exemptible under the *Privacy Act* sections 18, 19, 20 and 21, and subsections 22(1) to 22(3).

When adverse information is uncovered as a result of a law enforcement inquiry conducted by the Royal Canadian Mounted Police (RCMP) or police agency of jurisdiction, or a security assessment conducted by CSIS, the investigative body must be consulted to discuss parameters surrounding the disclosure of that information to the individual before the interview.

9. Decisions and Delegation

Deputy heads are accountable for rendering decisions to deny, revoke, or suspend pending an investigation, a security clearance or site access clearance. Deputy heads may formally delegate authority for the following decisions:

- Decisions to grant or grant with a security waiver, a security status or clearance;
- Decisions to deny or revoke a security status; and
- Decisions to suspend pending an investigation a security status or a security clearance.

Decisions to deny, suspend or revoke a security clearance cannot be delegated.

The results of security screening must support decisions regarding an individual's reliability, loyalty, and reliability as it relates to loyalty.

All decisions must be made on the basis of the quality, quantity, relevance and credibility of information and intelligence; an evaluation of any risks attached to making the appointment or assignment; and a judgment of whether such risks are acceptable in light of the nature and sensitivity of information to be accessed, the duties to be performed, and the operations of the department or agency.

In determining reliability, the question to be answered is whether the individual can be trusted to safeguard information, assets and facilities, and be relied upon not to abuse the trust that might be accorded and to perform the assigned duties in a manner that will reflect positively on and not pose a security risk to the Government of Canada. In other words, is there reasonable

cause to believe that the individual may steal or misuse valuables, exploit assets and information, fail to safeguard information and assets entrusted to him or her, or exhibit behaviour that would reflect negatively on his or her reliability.

In determining loyalty, the question to be answered is whether there is reasonable cause to believe that the individual has engaged, is engaged, or may engage, in activities that constitute a threat to the security of Canada as defined in the *Canadian Security Intelligence Service Act* and whether he or she has disclosed, may disclose or may be induced to disclose, or may cause to be disclosed in an unauthorized way, sensitive information.

10. Information to Support Decision Making

Decision making must be supported by an assessment from the official or organization responsible for conducting the security screening. Information must not be withheld from a deputy head, DSO or delegated official responsible for rendering a decision, unless prohibited by law, such as under the *Privacy Act,* the *Criminal Records Act* or other applicable legislation.

When no adverse information is uncovered, or when any doubt as to whether the individual can be trusted to safeguard information, assets or facilities is resolved, the individual can be granted the required security status or clearance.

11. Notification of a Decision to Grant

Individuals are notified of the decision to grant a security status or clearance through a formal process of conducting a security briefing to inform them of the decision and of their personal security responsibilities. Individuals are required to acknowledge their security responsibilities and a record of the decision and acknowledgement must be kept on their security screening file.

When a security clearance is granted, CSIS must be informed of the decision.

12. Temporary Access to Sensitive Information, Assets or Facilities

Situations may arise when there is an urgent or compelling need to temporarily provide an individual with access to sensitive information, assets or facilities that is beyond what their current security status or clearance allows them to access. In such cases, after assessing the risks associated with doing so, departments or agencies may decide to provide the individual temporary access to information, assets or facilities.

The granting of temporary access does not allow, under any circumstances, access to compartmented information or to information for which access is restricted in accordance with international agreements or special caveats. If such access is required, the associated security screening prerequisites and other requirements must first be complied with (e.g. access to a SIGINT compartment requires a Top Secret clearance and indoctrination in accordance with criteria established by the Communications Security Establishment Canada).

When temporary access is granted, departments and agencies must ensure that that access is controlled and that the individual receives a formal and detailed security briefing on his or her security responsibilities. These responsibilities must be formally documented; must specify the duration of the access; and must be attested to by the individual, the DSO or delegated official, and the custodian of the information to be accessed. The individual must be debriefed following the removal of temporary access and reminded of the continuing responsibility to maintain the confidentiality of the sensitive information to which he or she has had access. The briefing and debriefing must be conducted by the DSO or delegated official, and a copy of the signed agreement must be placed on the individual's security screening file.

Temporary access to classified information for urgent or compelling needs must be limited to less than four months. It is not to be used as a substitute for conducting the required security screening activities for the individual's status or clearance to be upgraded. Measures should be taken to initiate the upgrade process if it is expected that access may be required for longer than four months.

When determining their security screening requirements, departments and agencies should take measures to plan for short periods of absence (e.g., vacations, sick leave, training) to ensure that several individuals in each work unit are security screened to the highest level required based on duties and need to access sensitive information, and to ensure continuity of operations.

If unforeseen circumstances arise and it would not be financially or operationally practical to process a security screening at the higher level, consideration should be given to relying on an individual in another area of the department or agency who has the required security clearance to access to the sensitive information for the purpose of indicating whether immediate action is required, or for taking action, as appropriate. In respect of the need-to-know principle, these individuals must also be briefed and debriefed as described above.

13. Notification of a Decision to Grant with a Security Waiver

In limited circumstances, when security concerns are encountered during the course of security-screening individuals a department or agency has a demonstrated need to engage to perform duties that cannot be performed by others, a decision may be made to grant a security status or clearance subject to a security waiver.

A security waiver formally details restrictions attached to the granting of a security status or clearance that limit an individual's access to what is essential to perform the assigned duties. The waiver may include additional monitoring or reporting requirements to provide added assurance of an individual's ongoing reliability and/or loyalty to Canada.

A security waiver is not a substitute for the requirement to security-screen individuals at the level required by the position, and the decision to grant a security status or clearance with a waiver can only be made once the individual has undergone security screening.

Conditions specified in a security waiver may include, but are not limited to the following:

a. The department or agency may not allow non-Canadian citizens access to "Canadian eyes only" information unless it includes the person's country of citizenship (see "Foreign Nationals" below);
b. Subject to the provisions of any information-sharing agreements, the department or agency will not grant access to classified information from a foreign government without the written agreement of that foreign government;
c. The department or agency will not grant access to classified information from other departments or agencies without consultation with those departments or agencies;
d. The security status or clearance granted to the individual is not transferable to any other duty or position in the department or agency or to any other department or agency;
e. The department or agency will limit access to sensitive information to that required to perform the specific duty; and
f. Any other condition necessary to minimize the risk to the security of the department, agency or government as a whole.

Individuals are notified of the decision to grant a security status or clearance with a waiver through a formal process of conducting a security briefing. During that briefing, the individual is informed of the decision and of his or her security responsibilities, and signs the security waiver. Individuals are required to acknowledge their security responsibilities and a record of the decision and acknowledgement must be kept in their security screening file. The department or agency is to reassess the security waiver every year, at a minimum.

14. Foreign nationals

Foreign nationals who have not been granted a Government of Canada security clearance but who hold a valid security clearance granted by their national government may be eligible to access Canadian government security classified information and assets when their security clearance is recognized by the Canadian government in accordance with a formal arrangement. Such formal arrangements may include a national-level bilateral instrument or a bilateral instrument between individual Canadian and foreign government departments or agencies. The instrument must include provisions for the mutual recognition of security status or clearance and the handling and storage of security classified information and assets.

Departments and agencies must confirm with the security screening service provider whether a bilateral instrument is in effect.

Subject to the provisions of any information-sharing arrangements, a foreign national is not to access information from a third-party foreign government without the written agreement of that foreign government.

15. Review for Cause

A review for cause is a reassessment of an individual's eligibility to hold a security status or clearance previously granted. It is a formal process that is initiated when new information is uncovered or reported about an individual that may call into question their reliability and/or loyalty to Canada. A review for cause requires that an investigation and security interview be conducted (see below). When required, security screening may also be redone.

The review for cause of a security status or clearance and any subsequent decision does not constitute a form of disciplinary action. Rather, it is an administrative action that could result in the termination of an individual's employment, contract or assignment because a security status or clearance is a condition of employment, assignment or contract.

A review for cause may be conducted in parallel to a disciplinary action. In such situations, consultation with departmental or agency human resources management unit is paramount.

When an individual's security status or clearance is not reviewed as a result of actions or inactions that are subject to disciplinary measures, the individual remains eligible to hold a security status or clearance. A disciplinary decision is not to be recorded on the security file unless it relates to a security concern.

16. Suspend pending an investigation

A security status or clearance may be suspended pending an investigation of a suspected security breach when the presence of the employee at work poses a security risk or could undermine or impede the investigation. The decision to suspend a security status or clearance is not a determination that the individual is guilty or innocent, but rather that the presence of the individual in the department or agency represents a reasonably serious and immediate security risk to individuals, the department or agency, or the government as a whole. The individual will be suspended without pay.

The onus is on the department or agency to satisfy the existence of a security risk significant enough to warrant the temporary suspension of an individual's security status or clearance. The simple fact that a criminal charge has been laid may not be sufficient to meet that onus.

Before rendering a decision to suspend a security status or clearance pending an investigation, the DSO or the delegated official must first consult with the human resources management unit to ensure that the employer's labour relations obligations are considered and addressed. The employee should be informed in writing of the action to be taken, including the following:

a. The decision to suspend the security status or clearance pending an investigation;

b. The reasons the security status or clearance is being suspended;
c. Any mitigating circumstances and contributing factors that were taken into consideration in reaching this decision; and
d. The manner and time frame in which the suspension will be administered.

A fair and objective investigation must be conducted as expeditiously as possible. Access to information, assets or facilities must be prohibited, pending the completion of the investigation. The department or agency must show that it investigated the suspected security breach to the best of its abilities in a genuine attempt to assess the security risk of reinstating the individual. Departments and agencies must also consider, objectively, the possibility of reinstatement within a reasonable period of time following suspension in light of new facts or circumstances that may come to light during the course of the suspension. These matters, again, must be evaluated in consideration of the existence of a reasonable security risk to the legitimate interest of the department or agency or government as a whole.

17. Investigations and interviews

Investigations into an alleged security breach must be conducted as soon as possible after the relevant incident. Investigations must be conducted fairly and objectively, and should consider and provide the following:

a. Background information leading up to the relevant security incident or alleged misconduct;
b. Input from the witness or witnesses;
c. The employee's response to the allegation(s);
d. An analysis of the facts; and
e. The conclusion as to whether security has been breached.

In accordance with the principles of procedural fairness, employees should be informed of the alleged security breach and should be given an opportunity to respond. This opportunity is usually provided in the form of an interview, which normally takes place in private.

Individuals are to be notified of concerns leading up to a denial or revocation and are to be given an opportunity to respond to those concerns before a final decision is rendered.

18. Denial

When there is reasonable doubt as to an individual's reliability or loyalty to Canada, or whether the person can be trusted to safeguard sensitive information, assets or facilities, security status or clearance may be denied. A decision to deny a security status or clearance is made at the time the security screening is processed or when an upgrade is performed. In all cases, individuals must be informed in writing of the decision and of their rights of review or redress. They must also be prohibited from accessing sensitive information and assets.

19. Revocation

A revocation is an administrative decision to withdraw, following an update or a review for cause, the security status or clearance previously granted to an individual. A decision to revoke a security status or clearance may result in termination of employment or cancellation of a contract. The authority of the deputy head to revoke a security clearance cannot be delegated.

When a revocation is being considered for an employee, the DSO or delegated official is to consult the departmental or agency human resources management unit. When a revocation is being considered for a contractor, the contracting authority must be informed before the contractor is informed. If the individual concerned is on contract, the contract must be terminated. If the individual is an employee of a private organization or firm, the person can be replaced by another employee of that organization or firm who has a valid security status or clearance, otherwise the contract is to be terminated.

In all cases, individuals must be informed in writing of the decision and of their rights of review or redress. They must also be prohibited from accessing sensitive information and assets.

20. Notification of a Decision to Deny or Revoke

When a decision is made to deny or revoke an individual's security status or clearance, the DSO or delegated official, as appropriate, shall send, within 10 days after the decision is made, a written notice informing the individual of the decision. This notice will also include the reasons for the decision and the information on which the decision is based. The individual must be informed of his or her rights to redress. The letter may not involve full disclosure of information where issues of national security are involved or where such disclosure is not subject to disclosure under federal legislation.

When the decision to deny or revoke relates to a security clearance, the notification must come from the deputy head of the department or agency where the individual is employed.

Any dispute between the DSO or delegated official and the human resources management unit as to the appropriate action to be taken must be resolved before any action to deny or revoke a security status or clearance is taken.

Departments and agencies can consult the Treasury Board of Canada Secretariat and their department or agency's legal services unit about these matters and about the process of notification.

When a security clearance is denied or revoked, CSIS must also be informed of the decision.

Appendix E – Review and Rights of Redress

1. Procedural Fairness

When a review for cause is conducted or when a decision is being considered to deny or revoke a security status or clearance, departments and agencies must, while ensuring that the interests of government are protected, ensure that decisions are made using a fair procedure, and that actions and decisions are appropriate to the situation. Departments and agencies must be able to demonstrate and provide evidence that:

a. A fair and objective evaluation was conducted that respected the rights of the individual;
b. The individual was given an opportunity to explain potentially adverse information prior to rendering a decision;
c. The individual was briefed and given written reasons for the decision, unless the information is not to be disclosed under the *Privacy Act* or for reasons of national security; and
d. The individual was informed in writing of his or her right to redress and review.

2. Rights of Redress and Review

Any action or inaction that results in an individual not being granted a security status or clearance will negatively impact the individual and may have serious consequences, up to and including termination of employment or termination of a contract. Individuals who choose to have a decision reviewed may do so through the appropriate channels and must be informed in writing of the redress or review mechanisms available to them.

3. Challenging a Decision to Deny, Suspend or Revoke a Security Status

Employees who want to challenge a decision to deny, suspend or revoke a status may do so through the applicable grievance procedures or file a complaint with the Canadian Human Rights Commission if they believe that the decision was based on one or more prohibited grounds, as listed in the *Canadian Human Rights Act*.

Individuals from outside the public service, such as applicants and contractors, may complain to the Canadian Human Rights Commission or file an application for judicial review with the Federal Court, according to the specifics of each case.

4. Challenging a Decision to Deny or Revoke a Security Clearance

The *Canadian Security Intelligence Service Act*establishes the Security Intelligence Review Committee (SIRC) as the formal review body in cases concerning denial of a security clearance. Pursuant to Section 42 of the *Canadian Security Intelligence Service Act*, this right of review is available to outside candidates, employees and those contracting with the government who are denied a security clearance by a deputy head that results in:

a. An individual being denied employment, or being dismissed, demoted or transferred or being denied a promotion by reason only of a denial or a security clearance; or
b. An individual being denied a contract to provide goods or services to the Government of Canada by reason only of a denial of a security clearance.

When a deputy head disagrees with a SIRC recommendation to grant or reinstate a security clearance, the Office of the National Security Advisor, Privy Council Office (PCO), must be consulted before a final decision is made. The Chairperson of SIRC must also be informed in writing of the final decision taken by a deputy head in such cases.

5. Complaints to the Canadian Human Rights Commission

Any individual who is denied a security clearance may also file a complaint with the Canadian Human Rights Commission if the individual believes that the decision was based on one or more prohibited grounds, as listed in the *Canadian Human Rights Act*. If a minister advises the Commission that the basis of the denial relates to the security of Canada, the Commission may either dismiss the complaint or refer the matter to SIRC for investigation before proceeding.

Appendix F – Aftercare

1. General

The decision about an individual's eligibility for a security status or clearance that follows the initial security screening process reflects the person's eligibility at a specific point in time. That eligibility can change over time.

Aftercare practices are aimed at providing confidence in an individual's continued reliability and loyalty. Aftercare comprises formal, planned security briefings; security awareness; updates and upgrades; and the reporting of changes in circumstances, unusual contact or incidents. It also involves ongoing monitoring by departmental security officers (DSOs), delegated officials and managers of an individual's continued suitability to hold a security status or clearance.

These practices are essential to help build a culture of security, where individuals understand and implement security policies and practices to safeguard information, assets and facilities and to help ensure that security is not compromised, either negligently or unknowingly.

2. Standard Government of Canada Security Briefings

A security briefing is the last step of security screening and the first step of aftercare.

During a security briefing, individuals are informed of their security responsibilities under the *Policy on Government Security* and of the access permissions attached to their screening level. Security briefings provide an opportunity for people to ask questions and to develop a better understanding of these responsibilities. A security briefing formalizes the granting of the security status or clearance, as well as the individual's acceptance of and agreement to abide by the security responsibilities.

Security briefings are conducted at various times: before an individual takes up his or her duties, when required based on the update cycle, and whenever a change occurs in screening level.

3. Department and Agency Position-Specific Security Briefings

The standard security briefing covers general security requirements common to all individuals. Some departments and agencies may conduct briefings tailored to their operating and risk environment. Such briefings may provide specific details related to the protection of information, assets and facilities in the context of special duties, notably those related to security and intelligence.

4. Security Awareness

Security awareness is the practice of regularly reminding individuals of their security responsibilities and advising them of emerging issues and concerns.

Security awareness provides individuals with the knowledge and tools necessary to protect information, assets and facilities. Topics addressed through security awareness typically include the following:

a. Workplace security, including building access, the requirement to display security badges, and practices related to monitoring work-related behaviour through access controls;
b. Physical and information-technology security practices related to the proper handling, marking, transport, transmittal, storage and destruction of sensitive information or assets;
c. Emerging security concerns, including security threats from malware, phishing, or social engineering;
d. Minimizing risks inherent in working with sensitive information away from the official workplace (e.g., telework, mobile computing, travel);
e. Methods of coercion and strategies for collecting sensitive government information, and requirements to report security incidents and unusual contacts or contacts with foreign officials;
f. Obligations to report significant changes in personal circumstances that may warrant a review of the status or clearance granted; and
g. Consequences of failure to properly protect information, of circumventing security measures and of security breaches.

5. Updates

The purpose of an update is to reassess individuals' reliability and/or loyalty taking into account changes in their personal circumstances since the time they were last granted a security status or clearance. An update focuses on determining whether changes in personal circumstances pose a potential security risk in light of the duties being performed, and therefore affect eligibility to hold a security status or clearance. The established update cycles do not preclude an update from being done more frequently for cause.

When an update becomes six months overdue because an individual persistently delays providing the personal information necessary to conduct the security screening, consideration will be given to administratively cancelling the individual's security status or clearance until such time as he or she provides the required information. Administrative cancellation of an individual's security status or clearance means that the person no longer meets a condition of employment and could result in termination of employment or cancellation of a contract.

6. Upgrades

The purpose of an upgrade is to change the status or clearance to a higher level. Until the security screening activity required for the upgrade is completed and the higher level of security screening is officially granted, individuals cannot be provided access to higher levels of sensitive information, assets and facilities.

Temporary access may be granted when there is a need to access sensitive information at a higher level than what an individual's current security status or clearance permits (see Appendix D for details). Temporary access, however, is not to be used as a replacement for conducting an upgrade when the duties to be performed require it.

7. Reporting Changes in Behaviour and Security Concerns

The need to maintain a culture of security must be balanced with the need for people to trust that they are in a safe environment to do their work, and with individuals' legitimate expectation of privacy. Reporting changes in behaviour and security concerns must never be used as a way to increase personal power, to criticize an individual's work, or to cause embarrassment resulting from actions or thoughts. Departments and agencies must respect individuals' right to privacy, but must continue to assess their behaviour to identify changes or suspicious patterns that could give rise to security concerns.

Departments and agencies must ensure that individuals understand the reporting requirements detailed in the security screening certificate and briefing form, as well as any additional reporting requirements that may be established in departmental or agency procedures. This includes how to report changes or concerns and to whom they should be reported.

Managers, who are in contact with employees and contractors daily, are among the first people likely to recognize changes in behaviour. They are required to report these changes to the DSO or the delegated official.

Managers and employees should be trained so that they understand what they should be looking for and to ensure that they are vigilant. Unusual behaviour that may be cause for concern and should be reported to the DSO or delegated official include, but are not limited to, the following:

a. Drug or alcohol misuse;
b. Sudden or marked changes in financial situation or expenditures (e.g., bankruptcy, unexpected wealth);
c. Expressions of support for extremist views, actions or incidents, particularly when violence is advocated;
d. Unexplained hostile behaviour or communication;
e. Unexplained frequent absences;
f. Indications of fraudulent activity;
g. Disregard for safeguarding sensitive information or assets (e.g., violations, breaches of security); or
h. Persistent or unusual interest in or attempts to gain access to sensitive information, assets or facilities to which an individual has no work-related need to access.

8. Reporting Changes in Personal Circumstances

All individuals are required to report information related to a change in personal circumstances that may affect the security status or clearance they have been granted. Reporting requirements are detailed in the Security Screening Certificate and Briefing Form. At a minimum, individuals are required to report the following:

a. Change in criminal record status (criminal conviction, suspension of a criminal record, other judicial prohibitions);
b. Involvement with law enforcement (e.g., suspect in a criminal investigation, arrest); and
c. Association with criminals; and
d. Significant change in financial situation (e.g., bankruptcy, unexpected wealth).

Individuals who work in S&I organizations may be required to report additional changes in their personal or legal status, including a change in marital status.

9. Contact and Incident Reports

Persistent or unusual contact from another individual, or attempts by another individual to obtain access to sensitive information, assets or a facility without proper authorization must be documented and investigated. Such targeting can occur at all levels and ranks of a department or agency.

Most attempts to collect sensitive information or intelligence are subtle and often appear innocuous. The following situations are to be reported:

a. Unusual or persistent contact or any attempt by an unfamiliar individual to access information, assets or facilities;
b. Planned or unplanned contact with embassy or foreign government officials, foreign officials or foreign nationals in Canada or outside Canada, when such contact is outside of regular duties; and
c. Actual or potential security incidents or concerns.

10. Reactivation and Expiry

A security status may be reactivated within 2 years, and a security clearance may be reactivated within 12 months without the need to redo security screening when the following conditions apply:

a. An individual has terminated employment or taken a leave of absence with the government and subsequently returned, and there is no adverse information or a security waiver on file; or
b. Private sector individuals have terminated a government contract and subsequently entered into a new contract or require access to sensitive government information during a pre-contractual phase for the purpose of bidding.

In all cases, individuals will be required to account for their activities during the period of absence, as well as for the circumstances surrounding their departure. A security status or clearance will not be reactivated for any reason if the circumstances surrounding the departure involved a review for cause, a revocation or a suspension pending an investigation, or if the departure related to discipline for other reasons.

Once an individual's reactivation period has elapsed, and if there has been no activity on the file, the security status or clearance will expire. If the person wants to reintegrate into the federal government or participate in a government contract he or she will have to undergo an initial security screening process to meet the condition of employment or condition of a contract.

11. Transferability

When the security status or clearance required by the receiving department is at the same or lesser level as the one previously granted to an individual, the security status or clearance may be accepted by the receiving department or agency at par and should only be redone in the following situations:

a. The results are more than five years old;
b. There is evidence to suggest that the security screening was not previously done in accordance with this Standard;
c. There is a security waiver attached to the status or clearance;
d. Results of law enforcement inquiries or security assessments have been removed from the file; or
e. There is adverse information on file that may represent a security risk to the receiving department or agency.

When enhanced screening is required, security screening will be reviewed accordingly, and additional inquiries, verification or assessments may be conducted in accordance with the requirements of the status or clearance.

In all other cases, the security screening will be redone to ensure that the receiving department bases its decision on current and relevant security screening. DSOs or delegated officials must ensure that they obtain and review an incoming individual's security file before formally granting the required security status or clearance.

12. Termination of employment

Upon termination of employment, engagement or assignment, all individuals will receive a formal debriefing to remind them of their continuing responsibilities to maintain the confidentiality of the sensitive information to which they have had access. All authorities and access permissions are to be reclaimed, including identification and access badges, and physical and logical access keys. DSOs or delegated officials, in consultation with departmental human resource advisors, must develop procedures and ensure that debriefings and reclamations are scheduled and conducted as a component of the overall separation process. The Security Screening Certificate and Briefing Form will be used to record that termination procedures have been completed.