Government of Canada | Gouvernement du Canada

Policy on Government Security

Note to reader

The Policy on Government Security took effect on July 1, 2019. It replaced the Policy on Government Security that was in effect from July 1, 2009 to June 30, 2019.

Effective January 6, 2025, the Policy on Government Security has been amended to include a new authority, revise a requirement for deputy heads, revise references, add to the description of security screening, and include definitions.

The following sections have been amended or added:

- Section 2.3 relating to the delegation of authority to issue standards, mandatory procedures, and other appendices.
- Subsection 4.1.3 relating to delegation of the authority to deny, revoke or suspend security clearances.
- Section 8 to include updated references to legislation and related policy instruments.
- Appendix A.1 relating to security screening for the entire life cycle.

Appendix B to include definitions from the Standard on Security Screening into the Policy on Government Security. Some definitions have been amended and/or renamed to reflect updated concepts and

for plain language.

1. Effective date

1.1 This policy takes effect on July 1, 2019.

1.2 This policy replaces the Policy on Government Security, dated July 1, 2009.

1.3 Transitional considerations:

1.3.1 Subsection 4.1.5 of this policy will take effect on July 1, 2019, or on the scheduled date for the renewal of the department's security plan, whichever is later.

2. Authorities

2.1 This policy is issued pursuant to section 7 of the Financial Administration Act.

2.2 The Treasury Board has delegated to the President of the Treasury Board the authority to amend and rescind directives related to this policy, including standards, mandatory procedures and other appendices.

2.3 The Treasury Board has delegated to the President of the Treasury Board the authority to issue standards, mandatory procedures and other appendices.

3. Objectives and expected results

3.1 The objectives of this policy are as follows:

3.1.1 To effectively manage government security controls in support of the trusted delivery of Government of Canada programs and services and in support of the protection of information, individuals and assets; and

3.1.2 To provide assurance to Canadians, partners, oversight bodies and other stakeholders regarding security management in the Government of Canada.

3.2 The expected results of this policy are as follows:

3.2.1 Governance of government security controls within departments, with partners and across government will be effective, by fulfilling specified functions and successfully producing the intended result;

3.2.2 Access to advice, guidance and services, including secure internal enterprise services, will be enabled;

3.2.3 Deputy heads and central agencies will have and share information needed for informed decision-making on government security priorities and resources;

3.2.4 Risk-based and standardized security practices and controls will be implemented, monitored and maintained; and

3.2.5 Management of security events will be coordinated to enable adaptation to a dynamic threat environment.

4. Requirements

4.1 Deputy heads are responsible for the following:

4.1.1 Designating a chief security officer responsible to the deputy head or to the departmental executive committee to provide leadership, coordination and oversight for departmental security management activities;

4.1.2 Establishing the department's security governance, including responsibilities for security controls and authorities for security risk management decisions;

4.1.3 Ensuring that their authority to deny, revoke or suspend security clearances is only delegated to the *Chief Security Officer* or *Individuals designated by deputy heads of internal enterprise service organizations to oversee their internal enterprise service activities,* should the deputy head decide to delegate.

4.1.4 Identifying security and identity management requirements for all departmental programs and services, considering potential impacts on internal and external stakeholders;

4.1.5 Approving a three-year departmental security plan that is reviewed annually, sets out strategies for meeting departmental security requirements reflective of and contributing to government-wide security priorities, and addresses the security controls described in Appendix A;

4.1.6 Reviewing any residual security risk that exceeds established authorities for security risk management decisions;

4.1.7 Ensuring that security incidents and other security events are assessed, investigated, documented, acted on and reported to the appropriate authority and to affected stakeholders;

4.1.8 Responding to direction, advice and information requests issued by the Treasury Board of Canada Secretariat and the Privy Council Office regarding security events that require an immediate or coordinated government-wide action;

4.1.9 Establishing a written agreement when the department relies on or supports another department or organization to achieve government security objectives (see subsection 6.3 of this policy for application of this requirement); and

4.1.10 Investigating and acting when significant issues regarding policy compliance arise, and ensuring that appropriate remedial action is taken to address these issues.

4.2 Deputy heads of internal enterprise service organizations, which are departments or organizations that provide internal enterprise services to other government of Canada departments are responsible for the following:

4.2.1 Establishing governance, including designating one or more senior officials, to oversee security considerations in the provision of internal enterprise services;

4.2.2 Liaising with client departments and the Treasury Board of Canada Secretariat when identifying security requirements for internal enterprise services;

4.2.3 Examining and acting on issues regarding fulfillment of security requirements with affected stakeholders;

4.2.4 Conducting periodic reviews (every three years at a minimum) to assess the extent to which the services provided meet government-wide security needs; and

4.2.5 Investigating and acting when significant issues regarding policy compliance arise, and ensuring that appropriate remedial action is taken to address these issues.

4.3 Deputy heads of lead security agencies, which are described in subsection 5.2 of this policy, are responsible for the following:

4.3.1 Designating a senior official or officials to oversee their lead security agency activities under this policy;

4.3.2 Consulting with the government-wide security policy governance when identifying priorities for their lead security agency activities;

4.3.3 Exercising leadership and providing departments with advice and guidance on government security, in accordance with section 5 of this policy and the following general responsibilities:

4.3.3.1 Participating in government-wide security policy governance to assist in setting direction and priorities that align with national security objectives and other government priorities;

4.3.3.2 Providing advice to departments, and developing technical and operational guidance to support departments in policy implementation, in accordance with their mandate and in consultation with the Treasury Board of Canada Secretariat and the government-wide security policy governance;

4.3.3.3 Consulting with the Treasury Board of Canada Secretariat, Global Affairs Canada and other relevant lead security agencies and stakeholders when developing international agreements, treaties or other instruments that could potentially affect government-wide security management practices;

4.3.3.4 Participating in the analysis of threats, vulnerabilities, risks and security events; and sharing related findings with relevant stakeholders; and

4.3.3.5 Providing expertise and support for the development of Government of Canada security awareness and training curricula.

4.4 The Secretary of the Treasury Board is responsible for the following:

4.4.1 Establishing government-wide security policy governance to set strategic direction and priorities and coordinating security priorities, plans and activities government-wide;

4.4.2 Representing government-wide security needs in security governance for internal enterprise services;

4.4.3 Liaising with deputy heads and other senior officials on security issues, including security events that have potential government-wide impacts;

4.4.4 Liaising with other lead security agencies on matters of national security and emergency management; and

4.4.5 Establishing measures that support the capacity and development of the security functional community.

5. Roles of other government organizations

5.1 This section identifies key government organizations in relation to this policy. In and of itself, this section does not confer any authority.

5.2 This section identifies lead security agencies and/or internal enterprise service organizations that have a leadership and support role in relation to this policy and contribute to the achievement of government security policy objectives. The responsibilities of each organization are identified, in accordance with its mandate, including the principal internal enterprise services provided.

5.3 The Canadian Security Intelligence Service is responsible for the following:

5.3.1 Providing government-wide services in security screening;

5.3.2 Fulfilling government-wide functions by investigating and analyzing threats to the security of Canada and by providing

related reporting and advice to the Government of Canada; and

5.3.3 Maintaining a central registry for the retention of forms that designate persons permanently bound to secrecy under the Foreign Interference and Security of Information Act.

5.4 Communications Security Establishment Canada is responsible for the following:

5.4.1 Serving as the lead technical authority for information technology (IT) security, including the provision of leadership, advice, services and guidance for technical matters related to IT security

5.4.2 Helping to ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;

5.4.3 Fulfilling the following government-wide functions:

5.4.3.1 Identifying emerging cyber threats;

5.4.3.2 Defending government networks and systems; and

5.4.3.3 Protecting against, and mitigating potential impacts of, cyber security events;

5.4.4 Leading the development of trusted sources of supply for government and critical infrastructure, and mitigating the risk of untrusted equipment;

5.4.5 Serving as the national authority for communications security (COMSEC), including the procurement, distribution, control and use of cryptographic devices and encryption keying material for national security systems; and

5.4.6 Serving as Canada's national authority for signals intelligence (SIGINT).

5.5 National Defence is responsible for the following:

5.5.1 Fulfilling government-wide functions for scientific and technological security research, defence intelligence, and investigation of security threats to military systems;

5.5.2 Providing support to departments in relation to the protection of Government of Canada officials outside Canada, cyber security, and the provision of other security-related services;

5.5.3 Providing support to Public Safety Canada in relation to the continuity of constitutional government and domestic counterterrorism;

5.5.4 Serving as Canada's National Distribution Authority for NATO (North Atlantic Treaty Organization); and

5.5.5 Serving as Canada's national authority for Talent-Keyhole (TK) information.

5.6 Global Affairs Canada is responsible for the following:

5.6.1 Providing leadership, advice and guidance regarding security at missions abroad, and conducting Canada's

international relations on matters related to government security;

5.6.2 Fulfilling government-wide functions related to security developments abroad, and providing services to departments abroad to ensure security at missions; and

5.6.3 Serving as Canada's National Security Authority for NATO.

5.7 The Privy Council Office is responsible for the following:

5.7.1 Establishing policy direction for the security of Cabinet confidences;

5.7.2 Fulfilling the following government-wide functions:

5.7.2.1 Ensuring that national security objectives are reflected in government-wide security policy governance;

5.7.2.2 Providing advice and guidance on implementing security readiness levels in emergency and increased threat situations; and

5.7.2.3 Providing strategic leadership to coordinate responses to operational security matters facing the government that are of national, intergovernmental or international importance; and

5.7.3 Providing advice on recommendations from the Security Intelligence Review Committee regarding the security clearance of individuals.

5.8 Public Safety Canada is responsible for the following:

5.8.1 Providing leadership, technical advice and guidance for matters related to business continuity management;

5.8.2 Providing operational leadership for the coordination, information sharing and situational awareness relating to security events involving multiple Federal Departments or Agencies that may have government-wide, intergovernmental, critical infrastructure or national impacts;

5.8.3 Providing leadership in establishing the necessary arrangements for the continuity of constitutional government in the event of an emergency; and

5.8.4 Leading coordination and strategic policy-making on national security and national cyber security matters.

5.9 Public Services and Procurement Canada is responsible for the following:

5.9.1 Providing leadership, advice and guidance for matters related to contract security;

5.9.2 Supporting and fulfilling government-wide functions for issuing personal record identifiers (PRI) to departments and agencies and individual agency numbers (IAN) to agencies outside the federal public service, and maintaining the PRI and IAN systems;

5.9.3 Providing emergency procurement and emergency accommodation, and providing security services to help ensure the protection of sensitive information entrusted to Canadian and foreign industry;

5.9.4 Providing internal enterprise services for contract security, base building security for general-purpose office facilities under its custodial responsibility, and IT security in support of providing and managing certain government-wide applications; and

5.9.5 Serving as the government's national authority for industrial security, and in this capacity, serving as Canada's Designated Security Authority for NATO.

5.10 The Royal Canadian Mounted Police is responsible for the following:

5.10.1 Providing leadership, advice and guidance for matters related to physical security;

5.10.2 Fulfilling government-wide functions related to criminal threat intelligence and criminal investigations; and

5.10.3 Providing government-wide services related to security screening, technical surveillance countermeasures, and safeguarding of designated persons.

5.11 Shared Services Canada is responsible for the following:

5.11.1 Planning, designing, building, operating and maintaining effective, efficient and responsive enterprise IT security

infrastructure services to secure Government of Canada data and systems under its responsibility.

5.12 The Treasury Board of Canada Secretariat is responsible for the following:

5.12.1 Establishing and overseeing a whole-of-government approach to Security management as a key component of all management activities by ensuring the conduct of periodic reviews of the effectiveness of security support services, to provide assurance that they continue to meet the needs of the government as a whole;

5.12.2 Providing policy leadership, advice and guidance for all matters related to government Security;

5.12.3 Providing strategic policy oversight and coordination for the management of security events that may affect the government as a whole.

6. Application

6.1 The Policy on Government Security and its supporting instruments apply to departments as defined in section 2 and entities included in Schedules IV and V of the Financial Administration Act (FAA), unless excluded by specific acts, regulations or orders in council.

6.2 The heads of the following organizations are solely responsible for monitoring and ensuring compliance with this policy within their organizations:

- Office of the Auditor General of Canada

- Office of the Chief Electoral Officer
- Office of the Commissioner of Lobbying of Canada
- Office of the Commissioner of Official Languages
- Office of the Information Commissioner of Canada
- Office of the Privacy Commissioner of Canada
- Office of the Public Sector Integrity Commissioner of Canada

6.3 Subsection 4.1.9 of this policy applies only to interdepartmental agreements pursuant to subsection 29.2 of the *Financial Administration Act* and to arrangements with Crown corporations, other orders of government, the private sector or other entities that are not governed by this policy, where the department has the authority to enter into such an agreement or arrangement.

6.4 Ministers of the Crown, ministers, and Ministers of State are responsible for the security of their staff and offices and for the security of sensitive information and assets in their custody, as directed by the Prime Minister.

7. Consequences of non-compliance

7.1 For an outline of the consequences of non-compliance, refer to the Framework for Management of Compliance (Appendix C: Consequences for Institutions and Appendix D: Consequences for Individuals).

8. References

8.1 Legislation

- Access to Information Act
- Canada Labour Code
- Canada Occupational Health and Safety Regulations
- Canadian Charter of Rights and Freedoms
- Criminal Code
- Emergency Management Act
- Financial Administration Act
- Official Languages Act
- Privacy Act
- Public Service Employment Act
- Federal Public Sector Labour Relations and Employment Board Act
- Foreign Interference and Security of Information Act
- Security of Canada Information Disclosure Act

8.2 Related policy instruments

- Directive on Service and Digital
- Directive on the Management of Materiel
- Directive on the Management of Procurement
- Directive on the Management of Projects and Programmes
- Directive on the Management of Real Property
- Foundation Framework for Treasury Board Policies
- Framework for the Management of Compliance
- Framework for the Management of Risk
- Policy on People Management
- Policy on the Planning and Management of Investments
- Policy on Results
- Policy on Service and Digital
- Values and Ethics Code for the Public Sector

9. Enquiries

9.1 Members of the public may contact Treasury Board of Canada Secretariat Public Enquiries for information about this policy.

9.2 Individuals from departments should contact their departmental security management group for information about this policy.

9.3 Individuals from the departmental security group may contact the Security Policy Division at the Treasury Board of Canada Secretariat by email at SEC@tbs-sct.gc.ca for interpretation of any aspect of this policy.

Appendix A: Security Controls

This appendix describes the security controls that are mentioned in subsection 4.1.5 of this policy.

A.1 **Security screening** is conducted in a way that is effective, rigorous, consistent and fair, throughout all stages of the security screening life cyle to provide reasonable assurance that individuals can be trusted to safeguard government information and assets and can reliably conduct their work duties, and to enable transferability of security screening between departments.

A.2 **Information technology security** requirements, practices and controls are defined, documented, implemented, assessed, monitored and maintained throughout all stages of an information system’s life cycle to provide reasonable assurance that information systems can be trusted to adequately protect information, are used

in an acceptable manner, and support government programs, services and activities.

A.3 **Physical security** requirements, practices and controls are defined, documented, implemented, assessed, monitored and maintained throughout all stages of the real property and materiel management life cycles to provide reasonable assurance that individuals, information and assets are adequately protected, thereby supporting the delivery of government programs, services and activities.

A.4 **Business continuity management** is conducted systematically and comprehensively to provide reasonable assurance that in the event of a disruption, the department can maintain an acceptable level of delivery of critical services and activities, and can achieve the timely recovery of other services and activities.

A.5 **Information management security** requirements, practices and controls are defined, documented, implemented, assessed, monitored and maintained throughout all stages of the information life cycle to provide reasonable assurance that information is adequately protected in a manner that respects legal and other obligations and balances the risk of injury and threats with the cost of applying safeguards.

A.6 **Security requirements associated with contracts and other arrangements** are identified and documented, and related security controls are implemented and monitored throughout all stages of the contracting or arrangement process to provide reasonable assurance that information, individuals, assets and services associated with the contract or arrangement are adequately protected.

A.7 **Security event management** practices are defined, documented, implemented and maintained to monitor, respond to and report on threats, vulnerabilities, security incidents and other security events, and ensure that such activities are effectively coordinated within the department, with partners and government-wide, to manage potential impacts, support decision-making and enable the application of corrective actions.

A.8 **Security awareness and training** is conducted systematically and comprehensively to ensure that individuals are informed of their security responsibilities and maintain the necessary knowledge and skills to effectively carry out their functions, and to provide reasonable assurance that individuals will not knowingly compromise security and that they understand the potential consequences of not meeting their security responsibilities.

Appendix B: Definitions

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 or the reactivation period has elapsed. An administrative cancellation is not recorded as a denial or revocation.

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.

authoritative source (*source autorisée*)

A collection or registry of records maintained by an authority that meets established criteria.

base building security(*sécurité de l'immeuble de baseé*)

Security safeguards provided by a building custodian to protect the building's structure and supporting infrastructure.

compartmented information (*information cloisonnée*)

Information derived from sensitive sources and methods. Access to compartmented information is limited to Top Secret and/or Enhanced 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 known as control systems. Control systems define who may access the information, and under what conditions.

compromise (*compromission*)

A breach of government security. Includes but is not limited to:

- unauthorized access to, disclosure, modification, use, interruption, removal, or destruction of sensitive information or assets, causing a loss of confidentiality, integrity, availability or value;
- any action, conduct, threat or gesture of a person toward an employee in the workplace or an individual within federal facilities that caused harm or injury to that employee or individual; and
- an event causing a loss of integrity or availability of government services or activities.

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 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.

critical service or activity (*service ou activité critique*)

A service or activity whose disruption would result in a high or very high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the Government of Canada.

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.

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, and place of birth. Examples are records of birth, immigration or citizenship from an authority with the necessary jurisdiction.

government security (*sécurité du gouvernement*)

The assurance that:

- information and assets that support government programs are protected throughout their life cycle against threats to their confidentiality, integrity, availability or value;
- employees in the workplace and individuals within federal facilities are protected against actions, conduct, threats or gestures of persons that could cause them harm or injury;
- continuity of government operations can be maintained during situations that may disrupt normal operations; and
- the Government of Canada can maintain the delivery of programs and services in the presence of threats to their integrity or availability.

internal enterprise services (*services internes intégrés*)

A service provided by a Government of Canada department to other Government of Canada departments intended on a government-wide basis.

internal enterprise service organization (*organisation de services internes intégrés*)

A department or organization that provides internal enterprise services to other Government of Canada departments. This includes lead security agencies that deliver government-wide security services.

identity (*identité*)

A reference or designation used to distinguish a unique individual, organization or device.

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 connaître*)

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 their official duties.

other individuals (*autres particuliers*)

Any persons who is not an employee to whom the government may need to provide access to sensitive information or assets, or access to facilities.

residual risk (*risque résiduel*)

In the context of the Policy on Government Security, the level of security risk remaining after the application of security controls and other risk mitigation actions.

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, including taking the appropriate measures to prevent and protect against threats while enforcing Canadian statues and supporting Canada's national interests.

security assessment (*évaluation de sécurité*)

The ongoing process of evaluating security practices and controls to establish the extent to which they are implemented correctly, operating as intended, and achieving the desired outcome with respect to meeting defined security requirements.

security authorization(*autorisation de sécurité*)

The ongoing process of obtaining and maintaining a security risk management decision and to explicitly accept the related residual risk, based on the results of security assessment.

security categorization (*categorisation de sécurité*)

The process of assigning a security category to information resources, assets or services based on the degree of injury that could reasonably be expected to result from their compromise.

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 conditions (*conditions de sécurité*)

A condition(s) attached to the granting of a security status or clearance that details an individual's eligibility to access to sensitive information or assets, and facilities. Security conditions 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.

security control (*mesure de sécurité*)

A legal, administrative, operational or technical measure for satisfying security requirements. This term is synonymous with "safeguard."

security event (*événement lié à la sécurité*)

Any event, act, omission or situation that may be detrimental to government security, including threats, vulnerabilities and security incidents.

security function(*fonction de sécurité*)

Activity that directly supports the achievement of government security objectives, including security screening, information technology security, physical security, business continuity management, information management security, security in contracts and other arrangements, security event management, security awareness and training, and the overall management of security (including governance, planning, monitoring and reporting).

security incident (*incident de sécurité*)

Any event (or collection of events), act, omission or situation that has resulted in a compromise.

security practices (*pratiques de sécurité*)

Processes, procedures and standards that govern the implementation, monitoring and maintenance of security controls.

security requirement (*exigence en matière de sécurité*)

A requirement that must be satisfied in order to reduce security risks to an acceptable level and/or to meet statutory, regulatory, policy, contractual and other security obligations.

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 conditions, deny, or revoke a security status, security clearance or site access status or site access clearance.

security status (*cote de sécurité*)

The minimum level of security screening for positions requiring unsupervised access to Government of Canada information, assets, facilities or information technology systems. Security screening for reliability status appraises an individual's honesty and whether they can be trusted to protect the employer's interests. Reliability status may also be referred to herein as a security status.

senior official (*haut fonctionnaire*)

For the purposes of the Policy on Government Security, individuals designated by the deputy head in the departmental security governance as having overall responsibility for the security aspects of a program, service or activity area or for a security function. Senior officials may include program officials, chief financial officers, chief audit executives, chief information officers, chief privacy officers and other officials designated pursuant to a statutory requirement, Treasury Board policy or other

requirement. Senior officials also include individuals designated by the deputy heads of internal enterprise service organizations to oversee their internal enterprise service activities under the Policy on Government Security.

sensitive information or asset(*renseignement ou bien de nature délicate*)
Information or asset that if compromised would reasonably be expected to cause an injury. This includes all information that falls within the exemption or exclusion criteria under the Access to Information Act and the Privacy Act. This also includes controlled goods as well as other information and assets that have regulatory or statutory prohibitions and controls.

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.

threat (*menace*)
Any potential event or act, deliberate or unintentional, or natural hazard that could result in a compromise.

trusted digital identity (*identité numérique de confiance*)
An electronic representation of a person, used exclusively by that same person, to receive valued services and to carry out transactions with trust and confidence.

trust framework (*cadre de fiabilité*)
In the context of the Directive on Identity Management, a set of agreed on definitions, principles, conformance criteria, assessment approach, standards, and specifications.

vulnerability (*vulnérabilité*)
A factor that could increase susceptibility to compromise.

ISBN: 978-0-660-09914-9

Date modified: 2019-07-01