Treasury Board of Canada
Secretariat

Secrétariat du Conseil du Trésor
du Canada

Canada

Policy on Government Security

Published: Apr 01, 2012

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

Catalogue Number: BT39-22/2012E-PDF
ISBN: 978-0-660-09914-9

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 : Politique sur la sécurité du gouvernement

Policy on Government Security

1. Effective date

1.1 This policy takes effect on July 1, 2009.

1.2 This version of the policy incorporates updates effective April 1, 2012.

2. Application

2.1 This policy applies to:

- All departments within the meaning of Schedules I, I.1, II, IV and V of the *Financial Administration Act* (FAA), unless excluded by specific acts, regulations or Orders in Council.

3. Context

3.1 Government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. The extent to which government can ensure its own security directly affects its ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being and security of Canadians.

3.2 Security begins by establishing trust in interactions between government and Canadians and within government. In its interactions with the public when required, the government has a need to determine the identity of the individuals or institutions. Within government, there is a need to ensure that those having access to government information, assets and services are trustworthy, reliable and loyal. Consequently, a broad scope of government activities, ranging from safeguarding information and assets to delivering services, benefits and entitlements to responding to incidents and emergencies, rely upon this trust.

3.3 In a department, the management of security requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls involving prevention (mitigation), detection, response and recovery. The management of security intersects with other management functions including access to information, privacy, risk management, emergency and business continuity management, human resources, occupational health and safety, real property, materiel management, information management, information technology (IT) and finance. Security is achieved when it is supported by senior management—an integral component of strategic and operational planning—and embedded into departmental frameworks, culture, day-to-day operations and employee behaviours.

3.4 At a government-wide level, security threats, risks and incidents must be proactively managed to help protect the government's critical assets, information and services, as well as national security. Advice, guidance and services provided by lead security agencies support departments and government in maintaining acceptable levels of security while achieving strategic goals and service delivery imperatives.

3.5 The management of security is most effective when it is systematically woven into the business, programs and culture of a department and the public service as a whole.

3.6 Deputy heads are accountable for the effective implementation and governance of security and identity management within their departments and share responsibility for the security of government as a whole. This comprises the security of departmental personnel, including those working in or for offices of Ministers or Ministers of State, and departmental information, facilities and other assets.

3.7 Ministers of the Crown, ministers, and Ministers of State are responsible for the security of their staff and offices as well as the security of sensitive information and assets in their custody, as directed by the prime minister.

3.8 This policy is issued under section 7 of the FAA.

3.9 Treasury Board has delegated to the President of the Treasury Board the authority to amend directives that support the policy in the following subject areas:

- Departmental security management
- Identity management

and to issue and amend standards that support the policy in the following subject areas:

- Information and identity assurance
- Individual security screening
- Physical security
- IT Security
- Emergency and business continuity management
- Security in contracting

3.10 This policy is to be read in conjunction with the *Foundation Framework for Treasury Board Policies*, the *Directive on*

Departmental Security Management and the *Directive on Identity Management*.

4. Definitions

4.1 For definitions of terms used in this policy, refer to Appendix A—Definitions.

5. Policy statement

5.1 The objectives of this policy are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.

5.2 The expected results of this policy are:

- Information, assets and services are safeguarded from compromise and employees are protected against workplace violence;
- Governance structures, mechanisms and resources are in place to ensure effective and efficient management of security at both a departmental and government-wide level;
- Management of security incidents is effectively coordinated within departments and government-wide;
- Interoperability and information exchange are enabled through effective and consistent security and identity management practices; and
- Continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies.

6. Requirements

6.1 Deputy heads of all departments are responsible for:

6.1.1 Establishing a security program for the coordination and management of departmental security activities that:

a. Has a governance structure with clear accountabilities
b. Has defined objectives that are aligned with departmental and government-wide policies, priorities and plans; and
c. Is monitored, assessed and reported on to measure management efforts, resources and success toward achieving its expected results;

6.1.2 Appointing a departmental security officer (DSO) functionally responsible to the deputy head or to the departmental executive committee to manage the departmental security program (Note: The deputy head of a small department or agency (SDA) can assume the role of DSO);

6.1.3 Establishing a formal arrangement with the service provider when the role of the DSO is fulfilled by a third party (e.g., shared or clustered service provider or a portfolio department);

6.1.4 Approving the departmental security plan that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation;

6.1.5 Ensuring that managers at all levels integrate security and identity management requirements into plans, programs, activities and services;

6.1.6 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;

6.1.7 Ensuring that their authority to deny, revoke or suspend security clearances is not delegated;

6.1.8 Ensuring that when significant issues arise regarding policy compliance, allegations of misconduct, suspected criminal activity, security incidents, or workplace violence they are investigated, acted on and reported to the appropriate law enforcement authority, national security agency or lead security agency.

6.2 Deputy heads of lead security agencies are responsible for:

6.2.1 Providing departments with advice, guidance and services related to government security, consistent with their mandated responsibilities;

6.2.2 Appointing an executive or executives to coordinate and oversee the provision of support services to departments and to represent the deputy head to TBS in this regard; and

6.2.3 Ensuring that the security support services provided help government departments achieve and maintain an acceptable state of security and readiness and that those services remain aligned with government-wide policies, priorities and plans related to government security.

- A list of lead security agencies and details on the nature and scope of their responsibilities under this policy are found in Appendix B—Responsibilities of Lead Security Agencies.

6.3 Monitoring and reporting requirements

Within departments

- Deputy heads are responsible for ensuring that periodic reviews are conducted to assess whether the departmental security program is effective, whether the goals, strategic objectives and control objectives detailed in their departmental security plan were achieved and whether their departmental security plan remains appropriate to the needs of the department and the government as a whole.

By departments

- Deputy heads are responsible for reporting periodically to TBS, on the status and progress of implementation of this policy and on the results of ongoing performance measurement.

Lead security agencies

- In additional to monitoring and reporting on their departmental security program Deputy heads of lead security agencies are also responsible for:
- Ensuring that periodic reviews are conducted to assess the effectiveness of their security support services to ensure they continue to meet the needs of departments and the government as a whole; and
- Reporting on their activities under this policy through current government reporting mechanisms, e.g., Management, Resources and Results Structure (MRRS), departmental performance reports (DPR) and reports on plans and priorities (RPP).

Government-wide

- TBS is responsible for:
    - Monitoring compliance with this policy and the achievement of expected results in a variety of ways, including but not limited to MAF assessments, Treasury Board submissions, DPRs, RPPs, results of audits, evaluations and studies, and ongoing dialogue and committee work; and
    - Reviewing and reporting to Treasury Board on the effectiveness and implementation of this policy and its directives and standards at the five-year mark from the effective date of the policy. Where substantiated by risk analysis, TBS will also ensure an evaluation is conducted.

7. Consequences

7.1 The deputy head is responsible for ensuring appropriate remedial actions are taken to address issues regarding policy compliance, allegations of misconduct, suspected criminal activity or security incidents, including denying, revoking or suspending security clearances and reliability status, as appropriate.

7.2 If the Secretary of the Treasury Board determines that a department may not have complied with any requirement of this policy or its supporting directives or standards, the secretary of the Treasury Board may request that the deputy head:

7.2.1 Conduct an audit or a review, the cost of which will be paid from the department's reference level, to assess whether requirements of this policy or its supporting directives have been met; and/or

7.2.2 Take corrective actions and report back on the outcome.

7.2.3 Consequences of non-compliance with this policy and its supporting directives and standards or failure to take corrective actions requested by the secretary of the Treasury Board may include recommending to Treasury Board that measures deemed appropriate in the circumstances be imposed.

8. References

Legislation relevant to this policy includes the following:

- *Access to Information Act*
- *Canada Evidence Act*
- *Canada Labour Code*
- *Canada Occupational Health and Safety Regulations*
- *Canadian Charter of Rights and Freedoms*
- *Canadian Human Rights Act*
- *Canadian Security Intelligence Service Act*
- *Criminal Code*
- *Criminal Records Act*
- *Defence Production Act*
- *Department of Foreign Affairs and International Trade Act*
- *Emergency Management Act*
- *Federal Real Property and Federal Immovables Act*
- *Financial Administration Act*
- *Interpretation Act*
- *Library and Archives of Canada Act*
- *National Defence Act*
- *Privacy Act*

- *Public Servants Disclosure Protection Act*
- *Public Service Employment Act*
- *Public Service Labour Relations Act*
- *Royal Canadian Mounted Police Act*
- *Security of Information Act*
- *Statistics Act*
- *Youth Criminal Justice Act*

Treasury Board policies, directives and standards relevant to this policy include the following:

- *Access to Information, Policy on*
- *Communications Policy of the Government of Canada*
- *Contracting Policy*
- *Controlled Goods Directive*
- *Departmental Security Management, Directive on*
- *Evaluation, Policy on*
- *Identity Management, Directive on*
- *Information Management Roles and Responsibilities, Directive on*
- *Federal Identity Program*
- *Fire Protection, Investigation and Reporting, Policy on*
- *Foundation Framework for Treasury Board Policies*
- *Information and Technology, Policy Framework for*
- *Information Management, Policy on*
- *Integrated Risk Management Framework*
- *Internal Audit, Policy on*
- *Internal Controls, Policy*
- *Learning, Training, and Development, Policy on*
- *Long-term Capital Plans, Policy on*
- *Losses of Money and Offences and Other Illegal Acts Against the Crown, Policy on*
- *Management of Assets and Acquired Services, Policy Framework for the*
- *Management of Compensation, Policy Framework for the*
- *Management of Information Technology, Policy on*
- *Management of Materiel, Policy on*
- *Management of Real Property, Policy on*
- *Management, Resources and Results Structure, Policy on*
- *Occupational Safety and Health*
- *Official Languages for Human Resources Management, Policy on*
- *Official Languages Policy Framework*
- *Operational Security Standard—Business Continuity Planning (BCP) Program*
- *Operational Security Standard - Management of Information Technology Security (MITS)*
- *Operational Security Standard - Physical Security*
- *Personnel Security Standard*
- *Privacy Protection, Policy on*
- *Project Management Policy*
- *Risk Management, Policy on*
- *Security and Contracting Management Standard*
- *The Values and Ethics Code for the Public Service*

9. Enquiries

Please direct enquiries about this policy to your DSO. For interpretation of this policy, the DSO should contact:

Security and Identity Management Division
Chief Information Officer Branch
Treasury Board Secretariat
Ottawa ON K1A 0R5

Email: SIDM-SGID@tbs-sct.gc.ca
Telephone: (613) 946-5046
Fax: (613) 952-7232
Teletype: (613) 957-9090 (TBS)

Appendix A—Definitions

availability (*disponibilité*)
The state of being accessible and usable in a timely and reliable manner.

business continuity planning (*planification de la continuité des opérations*)

The development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets.

communications security (COMSEC) (*sécurité des communications (COMSEC)*)

The application of cryptographic security, transmission and emission security, physical security measures, operational practices and controls to deny unauthorized access to information derived from telecommunications and that ensure the authenticity of such telecommunications.

compromise (*compromission*)

The unauthorized access to, disclosure, destruction, removal, modification, use or interruption of assets or information.

confidentiality (*confidentialité*)

A characteristic applied to information to signify that it can only be disclosed to authorized individuals to prevent injury to national or other interests.

critical service (*service essentiel*)

A service whose compromise in terms of availability or integrity would result in a 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 (GC).

department (*ministère*)

All departments named in Schedule I, divisions or branches of the federal public administration set out in column I of Schedule I.1, corporations named in Schedule II, and portions of the federal public administration named in schedules IV and V of the Financial Administration Act (FAA), unless excluded by specific acts, regulations or Orders in Council.

deputy head (*administrateur général*)

Deputy Head as defined in section 11 of the *Financial Administrtion Act*, and in the case of the Canadian Forces the Chief of the Defence Staff.

emergency (*urgence*)

A present or imminent event, including IT incidents, that requires prompt coordination of actions to protect the health, safety or welfare of people, or to limit damage to assets or the environment.

emergency management (*gestion des urgences*)

The prevention and mitigation of, preparedness for, response to and recovery from emergencies.

executive (*cadre supérieure*)

An employee appointed to the executive group (EX-01 to EX-05 levels), i.e., director, director general, assistant deputy minister or equivalent.

identity (*identité*)

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

identity management (*gestion de l'identité*)

The set of principles, practices, processes and procedures used to realize an organization's mandate and its objectives related to identity.

interoperability (*interopérabilité*)

The ability of federal government departments to operate synergistically through consistent security and identity management practices.

national interest (*intérêt national*)

The security and the social, political and economic stability of Canada.

reliability status (*cote de fiabilité*)

Indicates the successful completion of reliability checks; allows regular access to government assets and with a need to know to PROTECTED information.

risk (*risque*)

The uncertainty that can create exposure to undesired future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to impede the achievement of an organization's objectives.

security clearance (*cote de sécurité*)

indicates successful completion of a security assessment; with a need to know, allows access to classified information. There are three Security Clearance levels: Confidential, Secret and Top Secret.

security control (*mesure de sécurité*)

An administrative, operational, technical, physical or legal measure for managing security risk. This term is synonymous with safeguard.

security incident (*incident de sécurité*)

Any workplace violence toward an employee or any act, event or omission that could result in the compromise of information, assets or services.

security screening (*filtrage de sécurité*)

Any measure resulting in a high level of assurance that an individual can be granted specific access privileges within the context of the federal government.

signals intelligence (SIGINT) (*renseignement électromagnétique – SIGINT*)

Technical information or intelligence composed of (individually or in combination) communications intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation signals intelligence (FISINT).

communications intelligence (*COMINT*)

Technical information or intelligence derived from the exploitation of communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those systems or networks by other than the intended recipient.

electronic intelligence (*ELINT*)

Technical information or intelligence derived from the collection, processing and analysis of electromagnetic non-communications emissions.

foreign instrumentation signals intelligence (*FISINT*)

Technical information or intelligence derived from the collection, processing and analysis of foreign instrumentation signals by other than the intended recipient.

situational awareness (*connaissance de la situation*)

Having insight into one's environment and circumstances to understand how events and actions will affect business objectives, both now and in the near future. Having complete, accurate, and current SA is essential in any domain where technological complexity, decision making, and the well-being of the public interact. Because incident management involves predictions and forecasts, SA in the area of IT requires an understanding of the interrelationships between critical services and information, safeguards supporting IT infrastructure and processes, and evolving threats.

sophisticated IT security incident (*incident complexe de sécurité des TI*)

An event, usually initiated by sophisticated threat actors, that is complicated to detect and recover from, causes harm to GC networks and systems, and affects the confidentiality, integrity and availability of information.

sophisticated IT security threat (*menace complexe à la sécurité des TI*)

An entity or entities that make use of advanced technologies and tradecraft to penetrate or bypass protective systems and security technologies without being detected.

threat (*menace*)

An event or act, deliberate or accidental, that could cause injury to people, information, assets or services.

vulnerability (*vulnérabilité*)

An inadequacy related to security that could increase susceptibility to compromise or injury.

workplace violence (*violence dans le lieu de travail*)

An action, conduct, threat or gesture that can reasonably be expected to cause harm, injury or illness to an employee in the workplace.

Appendix B—Responsibilities of Lead Security Agencies

Lead security agencies provide advice, guidance and services to support the day-to-day security operations of departments and enable government as a whole to effectively manage security activities, coordinate response to security incidents, and achieve and maintain an acceptable state of security and readiness. This appendix describes their responsibilities as they relate to their areas of expertise.

Treasury Board Secretariat (TBS) establishes and oversees a whole-of-government approach to security and identity management as a key component of all management activities and monitors the adequacy of services to support these activities and practices across government. TBS is responsible for:

- Establishing and maintaining interdepartmental security governance to exercise strategic oversight of government security and providing leadership and recommending priorities related to:
    - Government security policies and approaches to security community development,
    - Establishment of standards and designation of the necessary authorities for identifying and authenticating individuals internal and external to the GC,
    - Security services provided by lead security agencies, and
    - Incident management (including preparedness, mitigation, response, recovery and post-incident analysis activities related to security);
- Setting government-wide direction, establishing priorities, and defining and formalizing security and identity management requirements for the GC and departments;
- Setting government-wide direction and defining requirements for the personal record identifier (PRI) and the individual agency number (IAN);
- Providing guidance to lead security agencies on training and awareness strategies and coordinating training and awareness programs for the development of the security and identity communities, security practitioners, managers at all levels and other functional communities;
- Establishing and leading GC security and identity community forums and events to support departments in implementing the *Policy on Government Security;*
- Establishing service standards, in collaboration with lead security agencies, related to the provision of advice, guidance and services to support the implementation of the *Policy on Government Security* and monitor its progress toward achievement of desired outcomes;
- Maintaining close links with Public Safety Canada, monitoring and evaluating its information products to identify incidents that may have public service implications, and making recommendations concerning the activation of emergency and incident response plans;
- Providing direction and advice to lead security agencies and departments on the approach and implementation of measures for managing security incidents, including incidents affecting government security, operation of government IT systems and networks, service delivery and confidence in government; and
- Providing oversight of incident management to ensure the government's strategic objectives are maintained. This includes, but is not limited to, performing post-mortem reviews on incident management activities, tracking the status of after-incident action reports, and developing lessons learned.

Privy Council Office (PCO) advises and supports the prime minister and Cabinet on national security matters and coordinates the related activities of departments and agencies. PCO is responsible for:

- Providing government-wide policy direction on national security and intelligence priorities;
- Advising departments on strategies, mechanisms and activities required to develop, implement, evaluate and improve a fully integrated security system in the GC in support of national security objectives;
- Providing direction to Public Safety Canada to help resolve government security incidents and events that may affect national security;
- Providing direction and advice to departments and agencies on implementing security readiness levels in emergency and

increased threat situations;
- Supporting the Prime Minister in establishing candidates' fitness for office for public office positions and conducting security clearances for deputy heads;
- Providing direction and advice to departments and agencies on the level of security support to be provided to ministers, secretaries of State and parliamentary secretaries; and
- Establishing government policy on the security of Cabinet Confidences (i.e., Confidences of the Queen's Privy Council for Canada) and of records administered under the Cabinet Papers System and coordinating the investigation into unauthorized disclosure or other compromise of those documents.

Public Safety Canada (PS) coordinates activities related to emergencies (which include IT incidents) affecting the GC and provides leadership in the area of emergency management, which includes continuity of operations and IT incident management. PS is responsible for:

- Establishing policies, standards and programs for emergency management;
- Providing advice and guidance to departments in developing situational awareness through the identification of information, assets and facilities that support critical services and government operations and defining dependencies and interdependencies to:
    - Help improve the government's preparedness and response capability,
    - Manage emergencies, and
    - Support federal decision making;
- Providing advice and guidance to departments for the preparation, maintenance, testing and implementation of emergency management and business continuity plans;
- Providing central coordination for assessing emerging complex threats and developing and promoting comprehensive, coordinated approaches to address risks within the federal government and across Canada;
- Developing and implementing emergency management training and learning programs and strategies for federal communities;
- Sharing lessons learned and best practices with emergency management practitioners and facilitating the sharing of information within the GC and between the GC and its relevant partners;
- Coordinating the development of national and regional level emergency management exercises and providing advice and guidance to departments on those on exercises;
- Promoting awareness of emergency management matters and facilitating the sharing of information to enhance emergency and incident management;
- Issuing information, advice and guidance to the GC on emergency management;
- Representing the GC on regional, national and international initiatives related to emergency management;
- Communicating PCO direction requiring departments and agencies to implement a readiness level in response to security threats;
- Monitoring potential, imminent and actual emergencies, including those significantly affecting IT, advising other departments and TBS accordingly and coordinating the management of emergencies that affect or may affect services to Canadians, government operations or the effective functioning of government. Under this function, PS is responsible for:
- Monitoring threats to services to Canadians, government operations or the effective function of government, including but not limited to government networks, information systems and other critical infrastructure, issuing advice, guidance and situational awareness reports to departments on potential or actual emergencies and coordinating the GC response to and recovery from an emergency;
- Responding to requests from government departments for specific technical advice, guidance and information on IT incident response and recovery;
- Developing post-incident analysis and after-action reports and recommending actions to TBS and departments to mitigate future incidents; and
- Reporting to TBS throughout all phases of incident management with its analysis of events and incidents that have or may have affected services to Canadians, government operations or the effective functioning of government.

Communications Security Establishment Canada (CSEC) provides leadership and coordination for departmental activities that help ensure the protection of electronic information and information systems of importance and serves as the government's national authority for SIGINT and COMSEC. CSEC is responsible for:

- Developing, based on analysis of community needs and in partnership with TBS, policy instruments related to information technology (IT) security for approval by TBS;
- Developing, approving and promulgating COMSEC- and SIGINT-related policy instruments for classified information and developing guidelines and tools related to IT security;
- Coordinating the development and provision of training and awareness related to IT security, COMSEC and SIGINT to DSOs, security practitioners and, as required, other authorized individuals;
- Leading IT security-related interdepartmental committees and working groups and facilitating the sharing of information and collaboration across security communities;
- Collecting and reviewing IT security best practices and making recommendations to TBS and security governance committees to facilitate security policy improvements and collaboration among departments;
- Conducting research on IT security methods, technologies or common services and proposing solutions to TBS and governance committees to improve risk management and economies of scale in government;
- Authorizing special SIGINT compartment indoctrinations and maintaining a national inventory for personnel cleared and indoctrinated in SIGINT;
- Authorize the operation of IT systems and facilities handling SIGINT;
- Responding to and participate in the investigation or analysis of sophisticated IT security incidents, threats and vulnerabilities and acting on information collected or received from these investigations;
- Providing advice and guidance to departments on the:
    - Protection and distribution of SIGINT,

    - Use and application of IT security products, COMSEC devices, cryptographic measures and key management,
    - Certification of shared and common IT services, emerging IT security technologies, ITS architecture design, common ITS solutions, including secure use of commercial-off-the-shelf products, system and network security design, and security posture and vulnerability assessments,
    - Design and upgrade of GCIT infrastructures and their security interconnectivities
    - Application of IT access controls for confidentiality and integrity as well as threat detection and prevention, and
    - Certification of GC shared, common or federated IT services;
- Providing services to departments for:
    - Key management systems and related components for classified information,
    - Predicting, preventing and defending against sophisticated IT security incidents, threats and vulnerabilities,
    - Handling and mitigation of sophisticated IT security incidents,
    - Security architecture design for GC shared, common or federated initiatives,
    - IT security product assessment and/or approval for products in use in classified domain when deemed necessary,
    - Tailored engineering and operational support for information infrastructure projects of importance to the GC, and
    - IT systems and facilities certification and accreditation for handling SIGINT;
- Developing procurement vehicles, in partnership with the Department of Public Works and Government Services (PWGSC), for pre-qualified IT security products and services;
- Gathering, analyzing and facilitating the authorized sharing of consolidated IT security threat and vulnerability information with departments and with Public Safety Canada; and
- Representing the GC on national and international initiatives related to IT security and SIGINT.

Public Works and Government Services Canada (PWGSC) provides leadership and coordination of activities to help ensure the application of security safeguards through all phases of the contracting process within the scope of the industrial security program (ISP). It also provides services related to physical security respecting the PWGSC Real Property Program and common services related to IT security for increased efficiency and economy of the GC. PWGSC is responsible for:

- Delivering services within the scope of the Industrial Security Program, including:
    - Developing, based on analysis of community needs, in partnership with TBS, policy instruments, guidelines and tools related to security in contracting for approval by TBS;
    - Coordinating the development and provision of training and awareness related to security in contracting;
    - Leading interdepartmental committees and working groups for security in contracting to facilitate the sharing of information and collaboration across communities of practice;
    - Collecting and reviewing best practices related to security in contracting and making recommendations to TBS and security governance committees to facilitate security policy improvements and collaboration among departments;
    - Maintaining a database of private sector organizations and individuals that have been authorized to access classified and protected information and assets;
    - Carrying out roles pursuant to international agreements respecting industrial security;
    - Conducting security inspections of companies that have access to protected and classified information and assets of NATO allies or those who are registered with countries with which Canada has reciprocal Industrial Security Memoranda of Understanding;
    - Processing requests for visits when a security cleared individual must visit a government/commercial organization in Canada or abroad;
    - Performing the necessary security screening of private sector individuals and organizations that have access to protected and classified information and assets, including those participating in foreign contracts;
    - Ensuring compliance in those security contracts that afford industry access to government information and assets;
    - Controlling and managing COMSEC assets in private sector companies and providing screening clearances and inspections for COMSEC assets in private sector companies;
    - Representing the GC on national and international initiatives related to security in contracting and controlled goods;
- Delivering services related to IT security, including:
    - Providing common IT security services and other solutions to enable departments to exchange information with citizens, businesses and employees;
    - Ensuring the confidentiality, integrity and availability of common IT services provided to departments;
    - Gathering, analyzing, consolidating and facilitating the sharing of operational threat and vulnerability information related to common IT services and government IT critical infrastructure managed by PWGSC and communicating the information to Public Safety Canada and, as authorized, to departments;
- Delivering services related to physical security, including:
    - Providing base building security for general-purpose office accommodation for which PWGSC is the building custodian; and
    - Procuring security guard services from the Canadian Corps of Commissionaires under the National Master Standing Offer for Commissionaire Services or from other service providers as appropriate;
- Delivering other services, including:
    - Issuing unique personal record identifiers (PRI) to departments and agencies, and individual agency numbers (IAN) to agencies outside the federal public service, upon request;
    - Maintaining the PRI and IAN systems, under the direction and guidance of the Treasury Board Secretariat; and
    - Coordinating the procurement of goods and services for all government departments during emergencies

Canadian Security Intelligence Service (CSIS) collects, investigates, analyzes and retains information and intelligence that may be suspected of constituting threats to the security of Canada and provides security assessments to departments within its statutory mandate. CSIS is responsible for:

- Developing, based on analysis of community needs and in partnership with TBS, policy instruments, guidelines and tools related to personnel security screening for approval by TBS;

- Participating in the development of training and awareness related to personnel security screening;
- Conducting investigations and providing security assessments in support of personnel security screenings to appraise loyalty to Canada, and so far as it relates thereto, the reliability of an individual
- Maintaining a central index of security assessments and a national central registry of information and documentation that it receives on all persons who are "permanently bound to secrecy" as defined in the *Security of Information Act*;
- Providing intelligence reports and assessments to the government on threats to the security of Canada, including issues relating to terrorism, espionage, clandestine foreign-influenced activities and economic security, and assessments relating to cyber security to help ensure the protection of the GC's critical services and systems;
- Conducting comprehensive and integrated analysis of all available threat information to build situational awareness for governmental decision makers. Under this function, CSIS is required to:
    - Assemble and analyze intelligence about potential threats from a wide range of sources and make the results of that analysis available to all GC representatives requiring it (e.g., DSOs and security practitioners);
    - Support, through its assessments, the security postures to be developed by governmental first responders, which include police forces and emergency management organizations;
    - Provide a unified and comprehensive threat picture related to special events involving the GC;
    - Support comprehensive threat and risk assessments related to the protection of services to Canadians, government operations and confidence in government; and
    - Provide information to Public Safety Canada to aid in emergency and IT incident management.

Royal Canadian Mounted Police (RCMP) provides leadership and coordination for departmental activities that help ensure the physical protection of government information, assets, facilities and people and provides services related to crime prevention, personnel screening, policing, law enforcement and investigations. RCMP is responsible for:

- Developing, based on analysis of community needs, policy instruments, guidelines, and tools related to physical security for approval by TBS;
- Coordinating the development and provision of training and awareness related to physical security for DSOs, security practitioners and other functional communities (e.g., program managers, accommodation and materiel management specialists and contractors);
- Leading interdepartmental committees and working groups for physical security to facilitate the sharing of information and collaboration within the community of practice;
- Collecting and reviewing best practices for physical security and making recommendations to TBS and security governance committees to facilitate security policy improvements and collaboration among departments;
- Coordinating research on physical security and personnel security screening and proposing solutions to TBS and governance committees to enable government to better manage risks and improve economies of scale;
- Providing advice and guidance to departments on:
    - Physical protection of government documents, assets and facilities, including facilities design,
    - Physical security equipment, systems, procedures and countermeasures,
    - Application of physical access controls, media disposal and system monitoring, and
    - Major events;
- Providing services for:
    - Reviewing and advising on counter-technical intrusion detection,
    - Criminal investigations, including computer forensics and cyber crime,
    - Personnel security screening, including fingerprint and criminal records checks and, when there are reasonable grounds, conducting law enforcement assessments and advising departments on the results, and
    - Safeguarding designated persons from threats or acts of violence;
- Gathering, analyzing, consolidating and facilitating the sharing of operational threat and vulnerability information related to identity crime, physical security, cyber crime and other relevant criminal activity and communicating it to Public Safety Canada, TBS and, as authorized, departments; and
- Representing the GC on national and international initiatives related to crime prevention and physical security.

Library and Archives of Canada (LAC) provides leadership and coordinates among government departments to help ensure the preservation of government information and records. LAC is responsible for:

- Developing, based on analysis of community and government needs and in partnership with TBS and Public Safety Canada, guidelines and tools related to the management of information resources for business continuity purposes, for approval by TBS;
- Advising on the management of information resources for business continuity purposes for GC departments;
- Providing secure storage and management for the protection of the essential records of GC institutions during emergencies;
- Monitoring, reporting, and proposing joint strategies to acquire records at risk of serious damage or destruction that are essential for the continuity of GC operations and services in order to properly preserve them for the long term; and
- Participating in and advising on emergency response for the continuity of GC operations and services.

Department of Foreign Affairs and International Trade (DFAIT) is the lead department for conducting foreign relations and the NATO National Security Authority for Canada. DFAIT is responsible for:

- Arranging and coordinating physical security for GC employees and assets housed at Canadian diplomatic and consular missions abroad;
- Providing advice to departments and ensuring periodic and appropriate inspections of security arrangements for the protection and security of NATO's classified information in Canada;
- Arranging and coordinating security for official visitors at DFAIT facilities;
- Providing advice to departments to help ensureadequate safeguards for the transmittal and transport of assets abroad and security initiatives with foreign governments and international organizations;

- Providing diplomatic reporting and assessments to the government on political and other developments abroad that impact on the security of Canadian Government assets and personnel;
- Providing diplomatic courier services for secure movement and safeguarding of classified information and assets between Canada and missions abroad;
- Ensuring the confidentiality, integrity and availability of official communications transmitted by electronic means between departments and Canadian diplomatic missions abroad;
- Conducting personnel security screening of locally engaged staff and other government officialsnot falling within the mandate of the *Interdepartmental Memorandum of Understanding on Operations and Support at Missions Abroad*; and
- Coordinating activities at missions abroad during national or international emergencies.

Department of National Defence (DND) / Canadian Forces (CF)

DND / CF are responsible for:

- Providing military intelligence for threat and risk assessment purposes; and
- Arranging and coordinating security for any foreign military personnel visiting Canada or otherwise present at a defence facility.

Canada School of Public Service (CSPS)

CSPS is responsible for:

- Providing training and educational services to help ensure that all public service employees have the knowledge and skills they need to deliver results for Canadians; and
- Developing, delivering and regularly updating, in collaboration with TBS and lead security agencies, courses and programs that meet the needs of the functional security and identity management communities, assessing whether participants successfully complete them and reporting the results to TBS on an annual basis.