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

Policy Checklist - Chief Security Officer (CSO) Responsibilities

This guidance is meant to assist CSOs in fulfilling their accountabilities as set out in the *Policy on Government Security* (PGS). The policy and its supporting instruments apply[1] to departments as defined in section 2 and entities included in Schedules IV and V of the *Financial Administration Act* (FAA).

The 2019 PGS requires deputy heads (DH) to designate a CSO[2], whose role is to provide strategic department-wide senior level advice and leadership, as well as coordination and oversight for security management activities, including the eight security controls[3].

The *Directive on Security Management* (DSM) section 4.1 outlines CSO responsibilities in supporting a DH's PGS accountabilities. As the department's senior, strategic security risk advisor[4], CSOs fulfill their Security responsibilities by conducting the following activities:

Departmental Security Plan (DSP)

Deputy Head Accountability

- ➢ Approving the DSP (an annual review is required) that sets out strategies for meeting departmental security requirements (including addressing the PGS' eight security controls) reflective of, and contributing to, government-wide security priorities.

CSO Responsibilities

☐ Lead the departmental security function by defining, documenting, implementing, assessing, monitoring, and maintaining security requirements, practices, and controls

- ➢ Ensuring the eight security controls and related practices are in place, monitored and maintained.

☐ Oversee the development, implementation, and maintenance of the DSP, in collaboration with other senior officials and stakeholders

- ➢ Ensure the DSP:
  - is up to date and approved annually by the DH (3-year cycle),
  - provides an integrated view of departmental security threats, risks and requirements, including mitigating activities, and
  - includes strategies, priorities, responsibilities and timelines for maintaining, strengthening, monitoring and continuously improving security practices as they relate to the eight security controls.

☐ Report to the deputy head on progress in achieving the priorities defined in the DSP

- ➢ Annual reporting to the DH regarding priorities.
- ➢ Recommend changes to departmental security practices, security controls and priorities (as required).

Resources

- ➢ Departmental Security Plan Template
- ➢ PGS GCpedia Page

[1] Unless excluded by specific acts, regulations, or orders in council.
[2] As a reminder, delegated CSOs must provide their designation letter (duly signed by the DH) and their contact information to TBS Security Policy Division at SEC@tbs-sct.gc.ca within 4 weeks of their designation.
[3] The eight security controls are defined in the Policy on Government Security Appendix A: Security Controls.
[4] The CSO is accountable for related security risk management decisions.

Governance

Deputy Head Accountability

- Ensure establishment of the department's Security governance, including responsibilities for security controls and authorities for security risk management decisions.

CSO Responsibilities

☐ Oversee the development, implementation and maintenance of internal departmental security governance, which identifies responsibility for security functions and authorities for security risk management decisions.

☐ Ensure the DH is represented in GC Security Governance Committees by participating in setting government-wide security management direction.

- This includes GC Security and Readiness Committee (GCSRC), GC Enterprise Security Control Committee[5] (GC ESCC) and ADM Security Committee (ADM SC), as applicable.

Security Screening

Deputy Head Accountability

- Ensure that a decision to deny, revoke or suspend a security clearance (Secret, Top Secret, Site Access) is not delegated.
- Review any residual security screening risk that exceeds established authorities for security risk management decisions.
- Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues.

CSO Responsibilities

☐ Ensure security screening is conducted in a way that is effective, rigorous, consistent and fair to provide reasonable/continuous 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.

- Security screening must be conducted in accordance with the *Standard on Security Screening*.

☐ Oversee the establishment of department-wide processes to assess and document actions regarding residual security screening risks for the department's programs and services and their supporting resources.

- Corrective actions must be implemented to address deficiencies and gaps. Limitations should be tested and validated.

Information Technology Security

Deputy Head Accountability

- Review any residual information technology security risk that exceeds established authorities for security risk management decisions.
- Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues.

CSO Responsibilities

☐ Ensure 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.

[5] Chaired by TBS, GC ESCC membership includes Lead Security Agencies and Internal Enterprise Service Organizations.

☐ Oversee the establishment of department-wide processes to assess and document actions taken regarding residual information technology security risks for the department's programs and services and their supporting resources.

- Corrective actions must be implemented to address deficiencies and gaps. Limitations should be tested and validated.

Physical Security

Deputy Head Accountability

- Review any residual physical security risk that exceeds established authorities for security risk management decisions.
- Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues.

CSO Responsibilities

☐ Ensure 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.

- Departmental security practices for conducting facility security assessments and authorizations and security inspections of facilities, including those with higher security requirements must be defined and documented.

☐ Oversee the establishment of department-wide processes to assess and document actions taken regarding residual physical security risks for the department's programs and services and their supporting resources.

- Corrective actions must be implemented to address deficiencies and gaps. Limitations should be tested and validated.

Business Continuity Management

Deputy Head Accountability

- Review any residual business continuity management related risk that exceeds established authorities for security risk management decisions.
- Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues.

CSO Responsibilities

☐ Ensure 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.

- Departments and agencies must conduct regular testing[6] (i.e., every two years) of business continuity plans (BCPs) to ensure an acceptable state of preparedness, including functional systems testing[7].

☐ Oversee the establishment of department-wide processes to assess and document actions taken regarding residual business continuity management risks for the department's programs and services and their supporting resources.

- Corrective actions must be implemented to address deficiencies and gaps. Limitations should be tested and validated.

[6] Tests can include communication trees (direct call, text or email/reply), alternate site access and function capability, ability to access critical applications remotely; supplier's BCP capability, etc. Exercises can include workshops, table tops, drills or simulations.

[7] Functional testing includes drills, functional exercises and full-scale exercises.

Information Management Security

Deputy Head Accountability

- Review any residual information management security risk that exceeds established authorities for security risk management decisions.
- Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues.

CSO Responsibilities

☐ Ensure 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.

☐ Oversee the establishment of department-wide processes to assess and document actions taken regarding residual information management security risks for the department's programs and services and their supporting resources.

- Corrective actions must be implemented to address deficiencies and gaps. Limitations should be tested and validated.

Security Requirements Associated with Contracts and Other Arrangements

Deputy Head Accountability

- Establish written agreements with other organizations when receiving security services[8].
- Review any residual security risk associated with contracts and other arrangements that exceeds established authorities for security risk management decisions.
- Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues.

CSO Responsibilities

☐ Ensure security requirements associated with contracts[9] 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.

☐ Oversee the establishment of department-wide processes to assess and document actions regarding residual security in contracting risks for the department's programs and services and their supporting resources.

- Corrective actions must be implemented to address deficiencies, gaps, and limitations should be tested and validated.

☐ Verify that written agreements are in place when the organization provides security services to, or receives from, another department or organization.

- Applies only to interdepartmental agreements[10] pursuant to subsection 29.2 of the FAA, and to arrangements with Crown corporations, other orders of government, the private sector or other entities that are not governed by the PGS.
- Applies to contracts for the production or delivery of goods or services and to any other arrangement involving the sharing of sensitive information or assets with organizations[11] or individuals that do not fall under the application of the PGS.

[8] This includes services related to security screening, information technology security, physical security, business continuity management, information management security, contract security, base building security, event management and awareness and training.

[9] National security must be considered throughout the contracting or arrangement process (i.e., national security clauses in contribution agreements and supply chain). For contracts and other arrangements with suppliers, the Security Requirements Check List (SRCL) may assist in identifying requirements related to national security.

[10] Entity must have authority to enter into such agreements or arrangements.

[11] Includes other orders of government and academic or scientific partners.

Security Event Management

Deputy Head Accountability

- Ensure that security incidents and other security events are assessed, investigated, documented, acted on and reported to the appropriate authority and to affected stakeholders.
- Respond 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.
- Review any residual security event management related risk that exceeds established authorities for security risk management decisions.
- Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues.

CSO Responsibilities

☐ **Ensure 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.**

☐ **Oversee the establishment of department-wide processes to assess and document actions taken regarding residual security event management risks for the department's programs and services and their supporting resources.**

- Corrective actions must be implemented to address deficiencies and gaps. Limitations should be tested and validated.

☐ **Oversee the establishment of department-wide processes to monitor and ensure a coordinated response to, and reporting of, department-specific threats, vulnerabilities, security incidents and other security events.**

- Processes must include the identification of actions to address deficiencies.
- Security incidents and other security events of significance must be reported to the Treasury Board of Canada Secretariat by email at SEC@tbs-sct.gc.ca on a cyclical basis or on request, for the purposes of government-wide policy monitoring.
- Material privacy breaches must be reported to **both** of the following:
  - Office of the Privacy Commissioner of Canada by email at notification@priv.gc.ca; and
  - Treasury Board of Canada Secretariat by email at SEC@tbs-sct.gc.ca.

☐ **Ensure that any significant issues regarding policy compliance, suspected criminal activity, national security concerns or other security issues are assessed, investigated, documented, acted on and reported to the deputy head.**

- As required, issues are to be reported to the appropriate law enforcement authority and/or security and intelligence agency (see Appendix I: Standard on Security Event Reporting), and to affected stakeholders.
- As required, cooperating in any resulting criminal or other investigation(s).

☐ **Collaborate with other senior officials and other stakeholders to respond to direction, advice and information requests issued by the Treasury Board of Canada Secretariat as the Employer (including the Office of the Chief Human Resources Officer), the Privy Council Office and the Government Operations Centre (GOC) regarding security events that require an immediate or coordinated government-wide action.**

- Security incidents and events must be reported without delay to the GOC by telephone at 613-991-7000 or by e-mail at GOC-COG@ps-sp.gc.ca and to the Office of the Chief Security Officer, PCO by telephone at 613-960-4000 or by e-mail at CMC-CGC@pco-bcp.gc.ca
- Cyber security incidents and other security events related to information technology (IT) must be reported in accordance with the Government of Canada Cyber Security Event Management Plan (GC CSEMP).

Security Awareness and Training

Deputy Head Accountability

- Review any residual security awareness and training related risk that exceeds established authorities for security risk management decisions.
- Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues.

CSO Responsibilities

□ **Ensure 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.**

□ **Oversee the establishment of department-wide processes to assess and document actions taken regarding residual security awareness and training risks for the department's programs and services and their supporting resources.**

- Corrective actions must be implemented to address deficiencies and gaps. Limitations should be tested and validated.

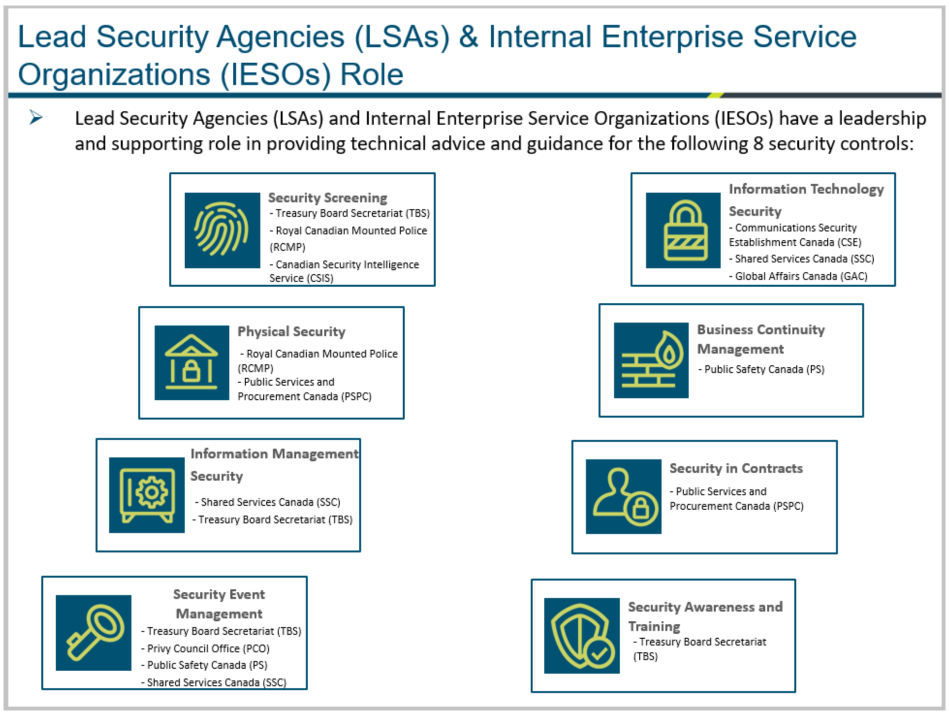
Appendix A - Lead Security Agencies and Internal Enterprise Service Organizations

The *Policy on Government Security* (PGS) identifies government organizations that have a key role in ensuring the trusted delivery of Government of Canada (GC) programs and services through effective security management in support of the protection of GC information, individuals and assets.

These Lead Security Agencies (LSAs) and/or Internal Enterprise Service Organizations[12] (IESOs) contribute to the achievement of government Security policy objectives by:

- Participating in government-wide security policy governance to assist in setting direction and priorities that align with national security objectives and other government priorities.
- Providing advice and developing technical and operational guidance to support departments in policy implementation.
- Providing secure internal enterprise services to other GC departments intended on a government-wide basis (identified IESOs only).
- Consulting with the Treasury Board of Canada Secretariat (TBS), Global Affairs Canada (GAC) and other relevant LSAs and stakeholders when developing international agreements, treaties or other instruments that could potentially affect government-wide security management practices.
- Participating in the analysis of threats, vulnerabilities, risks and security events; and sharing related findings with relevant stakeholders.
- Providing expertise and support for the development of GC security awareness and training curricula.

Figure 1: LSA and IESO Roles



Lead Security Agencies (LSAs) & Internal Enterprise Service Organizations (IESOs) Role

➢ Lead Security Agencies (LSAs) and Internal Enterprise Service Organizations (IESOs) have a leadership and supporting role in providing technical advice and guidance for the following 8 security controls:

Security Screening
- Treasury Board Secretariat (TBS)
- Royal Canadian Mounted Police (RCMP)
- Canadian Security Intelligence Service (CSIS)

Information Technology Security
- Communications Security Establishment Canada (CSE)
- Shared Services Canada (SSC)
- Global Affairs Canada (GAC)

Physical Security
- Royal Canadian Mounted Police (RCMP)
- Public Services and Procurement Canada (PSPC)

Business Continuity Management
- Public Safety Canada (PS)

Information Management Security
- Shared Services Canada (SSC)
- Treasury Board Secretariat (TBS)

Security in Contracts
- Public Services and Procurement Canada (PSPC)

Security Event Management
- Treasury Board Secretariat (TBS)
- Privy Council Office (PCO)
- Public Safety Canada (PS)
- Shared Services Canada (SSC)

Security Awareness and Training
- Treasury Board Secretariat (TBS)

Refer to section 5 of the PGS for additional information regarding LSA and IESO responsibilities.

LSA and IESO Contact information

Please refer to the GC Security Contact List to view contact information.

[12] A department or organization that provides internal enterprise services to other GC departments. This includes LSAs that deliver government-wide security services.

Appendix B - Additional Policy information, resources and tools

The *Policy on Government Security* (PGS) GCpedia website[13] provides security functional specialists with information, resources and tools related to the PGS.

Security Control Guidance

For each of the eight PGS security controls, Treasury Board Secretariat (TBS), Lead Security Agencies (LSAs) and Internal Enterprise Service Organizations (IESOs) share advice, guidance, and resources to support departments and agencies in their implementation.

Table 1 – Policy Guidance and Tools[14]

Security Screening	Physical Security	Information Technology security	Information Management security
• Appendix A: Mandatory Procedures for Security Screening Control • Position Analysis Tool (PAT) • Security Screening Toolkit • Security Screening Model File and Transferability 2020 • Personnel Security Screening Information Bank **LSA/IESO: TBS, RCMP, CSIS** • TBS Guidance • RCMP Guidance • CSIS Guidance	• Appendix C: Mandatory Procedures for Physical Security Control • Harmonized threat and risk assessment (TRA) methodology • Contract Security Manual • Guide to the Preparation of Physical Security Briefs **LSA/IESO: RCMP, PSPC** • RCMP Guidance • PSPC Guidance	• Appendix B: Mandatory Procedures for Information Technology Security Control • Patch Management Guidance • Guidance on Using Electronic Signatures **LSA/IESO: CSE, GAC, SSC** • CSE Guidance • CCCS Guidance • CCNSS Guidance • GAC Guidance • SSC Guidance	• Appendix E: Mandatory Procedures for Information Management Security Control • Directive on Security Management - Appendix J: Standard on Security Categorization • TBS - GC Categorization Model **LSA/IESO: SSC, TBS** • TBS Guidance
Business Continuity Management	**Security requirements associated with Contracts and Other Arrangements**	**Security Event management**	**Security Awareness and Training**
• Appendix D: Mandatory Procedures for Business Continuity Management Control • Guide for Developing a Business Continuity Management Program **LSA/IESO: PS** • PS Guidance	• Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control • Security Requirement Check List (SRCL) • Security requirements for contracting with the Government of Canada • Online Industrial Security Services	• Appendix G: Mandatory Procedures for Security Event Management Control • Appendix I: Standard on Security Event Reporting • Significant Event Information Sharing Protocol (December 2019) • Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019 • PCO - Operational Guidance on Security Readiness Levels (March 2020)	• Appendix H: Mandatory Procedures for Security Awareness and Training Control • SAWG-Security Awareness Resources • Security Awareness Employee Learning Tool **LSA/IESO: TBS** • TBS Guidance

[13] As a reminder, GCpedia is an essential internal knowledge sharing application tool for federal employees and is only accessible via Departmental network or VPN connection.

[14] Access and/or an account may be required to access resources available on GCpedia and GCconnex listed in the table.

	LSA/IESO: PSPC - PSPC Guidance	**LSA/IESO: PS, PCO, SSC and TBS** - PS Guidance - TBS Guidance - PCO Guidance	

Key Policy Enablers

Under the policy, Library and Archives Canada (LAC) and the Canada School of Public Service (CSPS) are identified as key policy enablers supporting government-wide security priorities and objectives. It is important to highlight that ongoing collaboration with central agencies, LSAs, IESOs, policy enablers and the Security functional community as well as their active participation in Security policy governance, as enablers, strengthens Government of Canada (GC) Security management.

TBS continues to work with CSPS to ensure departments are equipped with appropriate learning and training, and with small agencies to develop simplified guidance and tools tailored to their needs. This ensures security management practices within departments, with partners and government-wide is supported by modern, effective guidance, tools, learning and training opportunities.

Community Fora and Governance

Community fora provide Chief Security Officers (CSOs) and security functional specialists the opportunity to connect, collaborate and exchange information. These include the annual GC Security Summit, half-day GC Security Fora[15] held three times a year and other community engagement activities and events which encourage networking and sharing of best practices across the Security community. TBS continues to work with CSOs, LSAs and IESOs through established GC Security governance committees to strengthen and maintain mature Security management practices, and provide leadership, oversight and fora to address emerging security issues and concerns.

GC Security Governance currently includes the following committees:

- **Assistant Deputy Minister Security Committee (ADM SC):** Co-chaired by TBS and the Privy Council Office (PCO), the committee provides strategic direction and leadership regarding the development, implementation and ongoing evaluation of the PGS and operational readiness activities, supporting an integrated approach between LSAs, Internal Enterprise Service providers, Central Agencies and departments. Additional information, including the terms of reference may be found in the ADM SC GCconnex group page (membership required).

- **Government of Canada Security and Readiness Committee (GCSRC):** Co-chaired by TBS and the Privy Council Office (PCO), the committee acts as an advisory body to the ADM SC for the implementation of the GC Security Policy Suite and related readiness activities. Additional information, including the terms of reference may be found in the GCSRC GCconnex group page (membership required).

- **Government of Canada Enterprise Security Controls Committee (GC ESCC):** Chaired by TBS, the committee provides a forum for oversight, sharing of guidance and advice as LSAs/IESOs to ensure a consistent and integrated approach through risk mitigation strategies; informing security policy (through the LSA/IESO role), ongoing operations and engaging related communities of practice. Additional information, including the terms of reference may be found in the GC ESCC GCconnex group page (membership required).
- Government of Canada Security Summit (annual event)

[15] The GC Security Forum's previous meeting agendas and related materials are available on GCpedia.

In addition, ad hoc issues related to security policy, readiness and emergency management are discussed as relevant at the committees identified in Table 2.

Table 2 – GC Security Policy, Readiness and EM Governance

Area	Committee Name
Policy	• Public Service Management Advisory Committee (PSMAC) • Deputy Minister Enterprise Committee on Priorities and Planning (DM CEPP) • Assistant Deputy Minister Service and Enterprise Priorities Committee (ADM SEP)
Readiness	• Deputy Minister National Security Committee
Emergency	• Deputy Minister Emergency Management Committee (DM EMC)* • Assistant Deputy Minister Crisis Cell (ADM CC)* • Director General Emergency Management Committee (DG EMC)* • Director General Emergency Response Committee (DG ERC)*

**Supporting the GC response to the Covid-19 pandemic under the Federal Emergency Response Plan (FERP).*

Contact information

Library and Archives Canada (LAC)

- For additional information, please visit the Government Information Management and Disposition site.

Canada School of Public Service (CSPS)

- For additional information on learning content available to the security community, please visit the Security Functional Specialists page on GCcampus.

Canadian Centre for Cyber Security (CCCS)

- For additional information, you may visit the Cyber Centre's site or contact the Canadian Centre for Cyber Security (CCCS) by email at contact@cyber.gc.ca or by telephone at 1-833-292-3788.

Canadian Security Intelligence Service (CSIS)

- Integrated Terrorism Assessment Centre (ITAC)
  - You may contact the ITAC for any concerns related to the assessment of the terrorism threat to Canadians and Canadian interests abroad by email at ITAC1@smtp.gc.ca.

- National Security
  - You may contact the Canadian Security Intelligence Service (CSIS) for any national security related concerns by telephone at 613-993-9620.

- The Government Liaison Office (GLO) is the primary point of contact for the Service's Intelligence Assessments Branch (IAB), and CSOs can contact them by email at glo@smtp.gc.ca, for the following reasons:
  - For requests for Service information, including Threat Assessments
  - For requests for intelligence briefings (please note, they do not provide travel briefings)
  - For requests to be added to the dissemination list in order to receive Service assessment products
  - To provide feedback on Service assessment products

Centre for Labour and Employment Law (CLEL)

- The CLEL is responsible for providing labour and employment law legal advice directly to client departments and agencies. Please consult the CLEL contact list to find contact information for a representative or you may contact Christian.demers@justice.gc.ca or Nancy.paradis@justice.gc.ca.

Note: Requests for legal advice regarding Secret Clearances and revocations should be directed to Justice Canada.

Operation INTERSECT

- You may contact the INTERSECT operations team for any multi-jurisdictional and emergency preparedness/management related concern by email at intersect@ottawapolice.ca.

Public Safety (PS)

- Centre for Resiliency and Continuity Management (CRCM) Helpdesk
  - You may contact the Centre for Resiliency and Continuity Management (CRCM) Helpdesk for advice and guidance on the development and implementation of a CRCM program by email at crcm-cgcr@ps-sp.gc.ca.
- Government Operations Centre (GOC)
  - You may contact the PS Government Operations Centre (GOC) for any security event management related enquiry by email at goc-cog@ps-sp.gc.ca or by telephone at 613-991-7000.
- National and Cyber Security Policy
  - For additional information, please visit the PS National Security site or contact the Cyber Security Cooperation Program by email at CSCP-PCCS@ps-sp.gc.ca.

Public Services and Procurement Canada (PSPC)

- Base Building Security
  - You may contact PSPC Base Building Security for any enquiries related to physical security and base building security by email at TPSGC.securiteimmeubledebase-basebuildingsecurity.PWGSC@tpsgc-pwgsc.gc.ca.

- Contract Security Program (CSP)
  - You may contact PSPC CSP for any enquiries related to contract security requirements and screenings by email at ssi-iss@tpsgc-pwgsc.gc.ca, by telephone at 613-948-4176 or toll free at 1-866-368-4646. The information is also available on the Contract Security Program's client service centre web page.

- Controlled Goods Program (CGP)
  - You may contact PSPC CGP for any enquiries related to controlled goods that involve contractors by email at dmc-cgd@tpsgc-pwgsc.gc.ca, by telephone at 613-948-4176 or toll free at 1-866-368-4646.

Royal Canadian Mounted Police (RCMP)

- Canadian Criminal Real Time Identification Services (CCRTIS)
  - You may contact the RCMP CCRTIS for any concerns related to criminal record checks by email at CCRTIS-SCICTR@rcmp-grc.gc.ca.

- National Operations Centre (NOC)
  - You may contact the RCMP NOC for any national security related concerns by email at SIR-SIS@rcmp-grc.gc.ca or by telephone at 613-993-4460.

- Security Intelligence Background Section (SIBS)
  - You may contact the RCMP SIBS for any concerns related to law enforcement record checks by email at SIBSAdmin-SFSAdmin@rcmp-grc.gc.ca.

Privy Council Office (PCO)

- Crisis Management Cell (CMC)
  - You may contact the PCO CMC for any security event (including threats against ministers and PM) management related enquiries, for any National Security concern or when there is a change in your security readiness level by email at CMC-CGC@pco-bcp.gc.ca or by telephone at 613-960-4000.

- Security Centre of Excellence (SCoE)
  - You may contact the SCoE for any support you may need, from recruitment to professionalization, to operational questions from complex security screening to exercising your contingency plans by email at SCoE-CEeS-info@pco-bcp.gc.ca.
  - Young Security Professionals (YSP) Network
  - SCoE on GCcollab

Treasury Board Secretariat (TBS)

- Cyber Security Division
  - For additional information related to Cyber Security in the GC, please visit the Government of Canada Cyber Security gcxchange page or contact the Cyber Security Division directly for any cyber security related enquiry by email at ZZTBSCYBERS@tbs-sct.gc.ca.

- Digital Policy and Service Division
  - Contact the Digital Policy and Service Division for any enquiry related to the Policy on Service and Digital and related instruments at ServiceDigital-ServicesNumerique@tbs-sct.gc.ca.
  - Additional information can be found on the Service and Digital – GCpedia page.

- Access to Information Policy and Performance Division (AIPPD)
  - For additional information, please visit the Access to Information and Privacy (ATIP) Community GCpedia site or contact AIPPD for any enquiries related to the management and delivery of access to information programs, including legislative and policy compliance to the Access to Information Act by email at ippd-dpiprp@tbs-sct.gc.ca.

- Office of the Chief Human Resources Officer (OCHRO)
  - For additional information, please visit the Information for Government of Canada employees site or contact OCHRO directly at:
  - ohs-sst@tbs-sct.gc.ca for inquiries about occupational health and safety including workplace harassment and violence and related TBS instruments.
  - questions@tbs-sct.gc.ca for inquiries on any human resources matters.

- Security Policy Division
  - For additional information, please visit the PGS GCpedia site or contact the Security Policy Division by email at SEC@tbs-sct.gc.ca.

- Privacy and Data Protection Division (PDPD)
  - For additional information, please visit the ATIP Community GCpedia site or contact PDPD for any enquiries related to the management and delivery of privacy programs, including legislative and policy compliance to the Privacy Act at ippd-dpiprp@tbs-sct.gc.ca.