



Print version



DP 054

2007-10-16

INDUSTRIAL SECURITY PROGRAM

Table of Contents

1. [Background](#)
2. [Purpose](#)
3. [Policy](#)
4. [Scope](#)
5. [Definitions](#)
6. [Roles and Responsibilities](#)
7. [Guidelines](#)
8. [Compliance](#)
9. [References](#)
10. [Cancellation](#)
11. [Inquiries](#)

1. BACKGROUND

The [Government Security Policy](#) mandates departments to support the efforts to protect national interest and the Government of Canada's business objectives by safeguarding employees and assets while ensuring the continued delivery of services. Public Works and Government Services Canada (PWGSC), as a common service department for contracting, real property management, information technology and telecommunications, is assigned responsibility for overseeing the management of the [Controlled Goods Program](#) and the associated implementation of the [Controlled Goods Regulations](#), which is a domestic industrial security program, pursuant to the [Defence Production Act](#). PWGSC is also the Delegated Security Authority for Canadian and international industrial security responsibilities in accordance with the North Atlantic Treaty Organization's "Security within the NATO" C-M (2002) 49 and its Supporting Security Directives (AC/35-D/2000 through D/2005), and various bilateral and multinational industrial security arrangements.



2. PURPOSE

This departmental policy (DP) outlines the roles and responsibilities of PWGSC related to the [Industrial Security Program \(ISP\)](#). The ISP is composed of two service lines: contract security (provided by the Canadian and the International Industrial Security Directorates [CISD/IISD]) and controlled goods (provided by the [Controlled Goods Directorate](#)), both of which are administered by the Industrial Security Sector (ISS), Consulting, Information and Shared Services Branch (CISSB), PWGSC.



3. POLICY

In accordance with the [Government Security Policy](#), and pursuant to [Part 2 of the Defence Production Act](#), and the [Controlled Goods Regulations](#), Public Works and Government Services Canada shall:

1. administer the ISP;
2. provide advice to departments on the operational standards and technical documentation related to security in contracting. Security requirements are established by clients in the [Security Requirements Check List \(SRCL\)](#);

3. ensure compliance with international industrial security agreements, arrangements and memoranda of understanding;
4. develop the operational security standards technical documentation for security in government contracting.



4. SCOPE

This DP applies to all branches and special operating agencies (SOAs), both at headquarters and in the regions, and to all government programs or contracts and other arrangements administered by the Department.



5. DEFINITIONS

Breach of Security (*infraction à la sécurité*) means an action that results in the compromise of protected or classified assets (including information) or controlled goods.

Classified assets (*biens classifiés*) are assets whose unauthorized disclosure would reasonably be expected to cause injury to the national interest.

Classified contract (*contrat de nature délicate*) means any contract awarded to a private sector organization or individual involving access to CLASSIFIED information or assets.

Classified information (*renseignements classifiés*) means information related to the national interest that may qualify for an exemption or exclusion under the [Access to Information Act](#) or [Privacy Act](#) and the compromise of which would reasonably be expected to cause injury to the national interest.

COMSEC - Communications security (*COMSEC - sécurité des communications*) relates to cryptographic transmission and emission security measures applied to information stored, processed or transmitted electronically; a subset of information technology security.

Contracting process (*processus de passation de marchés*) includes bidding, negotiating, awarding, performance and termination of contracts.

Controlled Goods (*marchandises contrôlées*) are those military, strategic and military-related goods and technology, as well as dual-use goods and technology as included on the [Export Control List](#), which is administered by Foreign Affairs and International Trade Canada, specifically those goods listed in the Schedule to the [Export Control List](#) made under Section 3 of the [Export and Import Permits Act](#), more precisely:

Items listed under Group 2:

- Goods listed in item 2-1 that are prohibited firearms, as defined in paragraph (c) of the definition "prohibited firearm" in Subsection 84(1) of the [Criminal Code](#);
- Goods listed in item 2-3 that are ammunition with a calibre greater than 12.7mm;
- Goods listed in items 2-2 and 2-4 to 2-22;

Items listed under Group 5:

- Goods listed in item 5504; and

Items listed under Group 6:

- All goods listed.

[Controlled Goods Program](#) (*programme des marchandises contrôlées*) is a domestic industrial security program that helps strengthen Canada's defence trade controls through registration, prevention, deterrence and detection, and helps prevent the proliferation of weapons of mass destruction and of conventional weapons.

Designated Security Authority (*autorité désignée en matière de sécurité*) is responsible for developing, implementing, maintaining, coordinating and monitoring a security program consistent with the [Government Security Policy](#) and associated standards.

Examination (*examiner*) refers to the inspection of controlled goods by any means so as to provide a person with detailed

knowledge of the controlled goods' inherent properties and performance characteristics that would allow that person to use this knowledge so that the good could be reproduced or replicated, or the performance of a similar article could improve.

Industrial Security (*sécurité industrielle*) is a subset of national security concerned with the safeguarding afforded to Canadian and foreign CLASSIFIED and/or PROTECTED information and assets by private sector organizations and individuals.

National Interest (*intérêt national*) concerns the defence and maintenance of the social, political and economic stability of Canada.

NATO Security Committee (*Comité de la sécurité de l'OTAN*) is responsible for formulating NATO industrial security policy and making appropriate recommendations to the Council for the safeguarding of NATO classified information that is entrusted, or likely to be entrusted, to industry. This Committee considers matters of industrial security referred to it by the Council, a member nation, the Secretary General, the NATO Military Committee, Major NATO Commands and heads of NATO military and civil agencies.

Personal Information (*renseignements personnels*) means any information about an identifiable individual that is recorded in any form as defined in Section 3 of the [Privacy Act](#) including, without restricting the generality of the foregoing, race, age, marital status, education, medical, criminal, financial, employment records, identifying number, fingerprints, address, personal views, etc. Personal information does not include certain information concerning the position or functions of a government employee (para. 3(j)), the services performed by an individual under contract for a government institution (para. 3(k)), a discretionary benefit of a financial nature (para. 3(l)) and information about an individual who has been deceased for more than twenty years (para. 3(m)). Personal information is a subset of PROTECTED information.

Possess (*posséder*) means either actual possession, where the person has direct physical control over a controlled good at a given time, or constructive possession, where the person has the power and the intention at a given time to exercise control over a controlled good, either directly or through another person or persons.

Protected assets (*biens protégés*) are assets whose unauthorized disclosure would reasonably be expected to cause injury to a non-national interest.

Protected information (*renseignements protégés*) is information related to other than the national interest that may qualify for an exemption or exclusion under the [Access to Information Act](#) or [Privacy Act](#), and the compromise of which would reasonably be expected to cause injury to a non-national interest.

Registered person (*personne inscrite*) means an individual, corporation, partnership or any other business enterprise registered pursuant to the [Controlled Goods Regulations](#).

Secret (*secret*) is a level of classification that applies to information or assets which, when compromised, could reasonably be expected to cause serious injury to the national interest.

Top Secret (*très secret*) is a level of classification that applies to information or assets which, when compromised, could reasonably be expected to cause exceptionally grave injury to the national interest.

Transfer (*transférer*) means, in respect of a controlled good, to dispose of it or disclose its content in any manner.



6. ROLES AND RESPONSIBILITIES

1. The Deputy Minister is accountable for safeguarding sensitive information and assets under the ownership or control of PWGSC and for ensuring compliance with the [Controlled Goods Program](#).
2. The Assistant Deputy Minister, Consulting, Information and Shared Services Branch, (CISSB) is responsible for administering the ISP.
3. The Director General, Industrial Security Sector, CISSB, as the Designated Security Authority (DSA) for industrial security in Canada, is responsible for managing and directing an effective ISP in order to meet national, NATO and other international industrial security requirements.
4. The Director, Canadian Industrial Security Directorate (CISD), Industrial Security Sector (ISS), CISSB, is responsible for:

1. safeguarding client department and foreign government CLASSIFIED / PROTECTED information provided to the private sector under PWGSC contracts;
 2. managing a personnel security screening system for the Department and private sector organizations registered in the ISP;
 3. managing a facility security clearance system for private sector organizations registered in the ISP;
 4. granting security clearances and reliability status. Denying and revoking a reliability status;
 5. ensuring that breaches of industrial security are reported and investigated;
 6. ensuring that any breaches or violations of security relating to personal information are reported to the PWGSC Access to Information and Privacy Office and to the Departmental Security Officer;
 7. maintaining a database of private sector organizations and individuals that have been authorized to access CLASSIFIED and/or PROTECTED information and assets;
 8. providing industrial security education and training for contracting authorities and company security officers/authorized officials of private sector organizations;
 9. ensuring compliance with the [Government Security Policy](#) in contracts affording access to government CLASSIFIED and/or PROTECTED assets, when the contracting authority is PWGSC, or when requested by another department;
 10. on request, ensuring compliance with the [Government Security Policy](#) in contracts that are within delegated contracting responsibilities of departments, and affording access to government CLASSIFIED and/or PROTECTED assets.
5. The Director, International Industrial Security Directorate (IISD), ISS, CISSB, is responsible for:
1. negotiating and implementing international industrial security arrangements and memoranda of understanding with foreign countries, in consultation with both Foreign Affairs and International Trade Canada and ensuring their compliance in contracts that afford access to CLASSIFIED / PROTECTED foreign government information, and in contracts that afford foreign contractors access to CLASSIFIED / PROTECTED assets of the Government of Canada;
 2. managing the Canadian elements of the United States/Canada Joint Certification Program;
 3. managing the international industrial security document control system and NATO sub-registry;
 4. managing the international visit clearance system;
 5. ensuring that breaches of industrial security are reported to foreign industrial security officials;
 6. providing education and training on the document control and visit clearance systems to contracting authorities and company security officers/authorized officials of private sector organizations.
6. The Director, Program Harmonization and Services Directorate (PHSD), ISS, CISSB, is responsible for:
1. in consultation with the Treasury Board Secretariat, participating in the review of the [Government Security Policy](#) including instruments such as the [Security and Contracting Management Standard](#);
 2. reviewing and updating the [Industrial Security Manual](#);
 3. participating in the development/review of policies for the ISS Directorates.
7. The Director, Controlled Goods Program, ISS, CISSB, is responsible for:
-

1. safeguarding controlled goods through compliance enforcement of the provisions of [Part 2 of the Defence Production Act](#), and the [Controlled Goods Regulations](#);
 2. managing the [Controlled Goods Program](#), including interdepartmental, national and international relations, with other agencies;
 3. managing the registration and exemption requirements arising out of the various provisions of the [Defence Production Act](#) and the [Controlled Goods Regulations](#);
 4. ensuring that breaches of controlled goods security are reported, investigated and corrective measures taken to prevent recurrence;
 5. developing and implementing inspection and investigation standards;
 6. ensuring compliance with the [Controlled Goods Program](#) policies in all areas of activity, in particular the production, access, use or disposal of controlled goods and controlled goods information;
 7. maintaining a database of registered or exempt persons, with such database being available for consultation by registered private enterprises and public agencies;
 8. undertaking appropriate outreach activities to ensure awareness of the program and its objectives;
 9. ensuring ongoing communications as warranted with designated officials of registered persons (individual, corporation, partnership or any other business enterprise) under the [Controlled Goods Program](#).
8. The Director, Information Technology Security (ITS), Information Technology Services Branch (ITSB), is responsible for providing the Industrial Security Sector information technology security advice and assistance in support of the Industrial Security Program.
9. The PWGSC Contracting Authorities are responsible for:
1. specifying the necessary security requirement in the terms and conditions section of the contractual documentation;
 2. ensuring that contract documentation contains the necessary security clauses for the safeguarding of government assets, including IT systems;
 3. confirming with CISD that prospective contractors meet contract security requirements prior to being given access to CLASSIFIED and/or PROTECTED information and assets and prior to the award of CLASSIFIED and/or PROTECTED contracts;
 4. confirming that prospective contractors are registered, exempt or excluded under Part 2 of the [Defence Production Act](#) prior to their having access to controlled goods;
 5. ensuring the screening of private sector organizations and individuals who have access to PROTECTED or CLASSIFIED information and assets, as specified in the standards;
 6. ensuring that persons are appropriately registered, exempt or excluded from registration under the [Controlled Goods Program](#), before accessing controlled goods.



7. GUIDELINES

The [Controlled Goods Program](#) is set out in Parts 2 (Regulation of Access to Controlled Goods) and 3 (Offence and Punishment) of the [Defence Production Act](#), and the [Controlled Goods Regulations](#).

In summary, the legislation:

1. prohibits the possession, examination and transfer of controlled goods except by persons registered for those purposes, or exempt from registration;

2. lays out the rules for the registration of persons accessing (examination, possession and transfer of) controlled goods and the security conditions registered persons are required to adhere to, under the [Controlled Goods Regulations](#), for the safeguarding of controlled goods;
3. provides for the exclusion of persons (certain government and Crown Corporation employees) from Part 2 of the [Defence Production Act](#), and for rules of exemption from registration (foreign temporary workers and visitors);
4. provides for on-site inspections for the purpose of ensuring registered persons are meeting the security conditions required by the legislation;
5. provides for stringent penalties for persons who violate the [Defence Production Act](#) and/or the [Controlled Goods Regulations](#).



8. COMPLIANCE

Compliance with this DP is mandatory in accordance with the [Government Security Policy](#), NATO's C-M (2002) 49 "Security within the NATO" and its Supporting Security Directives (AC/35-D/2000 through D/2005), bilateral and multinational industrial security arrangements, memoranda of understanding, the [Defence Production Act](#), the [Export Control List](#) and the [Controlled Goods Regulations](#).



9. REFERENCES

Acts and Regulations:

- [Access to Information Act:](#)
- [Canada Labour Code:](#)
- [Canadian Charter of Rights and Freedoms:](#)
- [Canadian Security Intelligence Service Act:](#)
- [Controlled Goods Regulations:](#)
- [Criminal Code:](#)
- [Criminal Records Act:](#)
- [Defence Production Act:](#)
- [Emergency Preparedness Act:](#)
- [Export and Import Permits Act:](#)
- [Financial Administration Act:](#)
- [Interpretation Act:](#)
- [National Defence Act:](#)
- [Personal Information Protection and Electronic Documents Act:](#)
- [Privacy Act:](#)
- [Public Service Employment Act:](#)
- [Public Service Labour Relations Act.](#)

Treasury Board Publications:

- [Access to Information Guidelines:](#)
- [Government Security Policy:](#)
- [Privacy and Data Protection Policy.](#)

PWGSC Publications:

- [Departmental Consolidated Information and Asset Classification and Designation Guide:](#)
- [DP 051 - Departmental Security Program:](#)
- [DP 093 - Policy on the Handling of Contract Security Incidents:](#)
- [DP 104 - Policy on Information Technology Security:](#)
- [Industrial Security Manual.](#)

NATO Publication:

- NATO's C-M (2002) 49 "Security within the NATO" and its Supporting Security Directives (AC/35-D/2000 through

D/2005).

Other Documents:

- Bilateral and multinational industrial security arrangements and memoranda of understanding (CISD/IISD/PWGSC);
- [Export Control List](#).



10. CANCELLATION

This policy supersedes DP 054 dated 1997-08-11.



11. INQUIRIES

Director General
Industrial Security Sector
Consulting, Information and Shared Services Branch
Telephone: 613 -948 -1776

Original Signed by
François Guimont

François Guimont
Deputy Minister and
Deputy Receiver General for Canada

