Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada

CONTROLLED GOODS DIRECTORATE

POLICY GUIDELINE ON SECURITY PLANS

Canada

TABLE OF CONTENTS

1 INTRODUCTION

As conditions of registration under the Controlled Goods Directorate (CGD), a registered person must establish and implement a security plan and report without delay any security breach to the CGD.

2 OBJECTIVE

This policy guideline lays out the requirements under the *Controlled Good Regulations (CGR)* for establishing and implementing a security plan.

3 POLICY RATIONALE

An effective security plan at the place of business where controlled goods and/or controlled technology are kept ensures the adequate protection and transfer of those goods.

Controlled goods, as listed in the schedule to the Defence Production Act (DPA), are those military, strategic and military-related goods and technology, as well as dual-use goods and technology as identified in Group 2 (most items), item 5504 and Group 6 (all items) of the Export Control List (ECL) made under the authority of the Export and Import Permits Act (EIPA), administered by International Trade Canada. Items such as military vehicles, certain firearms and related ammunition, military aircraft, military electronics, missiles, satellites and most related components are generally considered to be controlled goods and/or controlled technology.

More detail on what constitutes considered to be controlled goods and/or controlled technology

4 POLICY GUIDELINE ON THE REGULATORY CRITERIA

As conditions of registration, every registered person is subject to the requirements to establish and implement a security plan and to advise the CGD without delay of any security breach in relation to controlled goods and/or controlled technology.

Reference: paragraphs 10(e) and (h) of the CG Regulations and section 40 of the *Defence Production Act*. See Appendix 1 for legislative text.

There must be a security plan at each place of business in Canada where controlled goods and/or controlled technology are kept. If the person operates a business at more than one geographical location or site, each location or site is to be treated as a separate place of business and a security plan is required for each location or site where controlled goods and/or controlled technology are kept.

A security plan not only has to be implemented and maintained, it also has to be effectively applied over the period of registration.

The security plan must be in writing, which means in typed format that is easily readable for those party to the implementation and application of the security plan. The plan can also be in electronic format for access from computer screens, as long as it is secure from amendment by unauthorized sources.

Each registered person is uniquely placed to determine the security plan they require in light of the nature of the controlled goods and/or controlled technology they access (possess, examine, transfer). Controlled goods are to be afforded a sufficient level of protection to prevent their unauthorized examination, possession or transfer.

A security risk management assessment is recommended as part of the determination required to put in place an effective security plan (see section 6 of this policy guideline).

As required by the CG Regulations, the written measures of a security plan need to set out all of the following:

1. The procedures used by the registered person to control the examination, possession and transfer of controlled goods and/or controlled technology.

2. The procedures for reporting and investigating security breaches in relation to controlled goods and/or controlled technology (see section 5 for further guidelines).

3. The description of the responsibilities of the registered person's security organization and the identity of individuals who are responsible for the security of controlled goods and/or controlled technology.

4. The contents of security briefings and training programs given to visitors, officers, directors, employees and temporary workers. (The provision of briefings and training programs will be the subject of a separate policy guideline).

5 SECURITY BREACHES

It is a condition of registration under the CG Regulations that the registered person must advise the CGD, without delay, of any security breach in relation to controlled goods and/or controlled technology.

Security breaches must be properly investigated by the registered person’s security organization and corrective action taken to prevent any re-occurrence. The registered person’s security organization is best placed to determine the nature of a security incident and whether it constitutes a breach as described below.

Security breaches can be categorized as follows: destruction, modification, removal or disclosure, of controlled goods and/or controlled technology.

The following list is provided as examples of security breaches:

- Loss of a controlled good - (known theft or disappearance)
- Unauthorized access to a controlled good
- Appearance of willful damage to a controlled good
- Appearance of willful tampering of a controlled good
- Witnessing of unauthorized persons examining controlled goods
- Transfer of a controlled good (including information format) to an unauthorized person

Any breach of a criminal nature that can be subject to conviction under the Criminal Code (such as theft), must be reported immediately to the appropriate criminal police body or agency, and in turn without delay to the CGD.

CGD is to be advised of a security breach via:
Telephone: 1 866 368-4646
Facsimile: (613) 948-1722
Electronic mail: ncr.cgd@pwgsc.gc.ca

Early advising of a security breach to the CGD allows for tracking and follow up. A follow up report from the registered person detailing the investigation and subsequent conclusions is to be forwarded to the CGD at either the e-mail address above or the following mailing address:

Director, Controlled Goods Directorate
c/o Central Mail Room
Place du Portage, Phase III OB3
11 Laurier Street, Gatineau
2745 Iris Street
3rd Floor Ottawa, Ontario
K1A 0S5

6 SECURITY RISK MANAGEMENT

Each registered person is uniquely placed to determine, in light of the controlled goods they possess, the security plan that is needed to adequately safeguard the controlled goods.

A security risk management assessment is recommended in the development of a security plan. Such assessment provides the cornerstone of an effective security plan. The most common tool used is a threat and risk assessment (TRA). A TRA consists of a four-step process for analyzing the security requirements needed to safeguard controlled goods and implementing sound security measures:

- Identification of the controlled goods
- Identification of possible threats of security breaches
- Assessment of the risks of such threats
- Implementation of adequate security measures, i.e. an effective security plan.

These four steps are explained further below.

1. **Identification of the Controlled Goods**. The registered person needs to determine the nature and location of the controlled goods and/or controlled technology. (This will also be the subject of a separate policy guideline on record keeping).

2. **Identification of Possible Threats of Security Breaches**. In identifying possible threats, controlled goods and/or controlled technology susceptible to theft, willful damage or unauthorized transfer must be taken into consideration. This should be derived from knowledge of the registered person's business, the environment in which the controlled goods are located and the activities of the individuals who will be examining, possessing or transferring those goods. After identifying the possible threats, they should be evaluated as to their likelihood and the consequences of their occurrence. This evaluation will help determine whether or not further protective security measures are required or justified.

3. **Assess the Risks of Security Breach Threats.** Examine all of the physical security measures in place at each place of business where controlled goods and/or controlled technology are kept, and evaluate their adequacy in preventing identified threats from occurring.

4. **Implement Adequate Security Measures**. After considering the areas susceptible to security breaches and their consequences, implement adequate security measures to optimize response to the threats and prevent the unauthorized transfer of controlled goods and/or controlled technology. Security measures proposed/implemented should take into consideration the nature of the controlled good being accessed by the registered person.

For comprehensive material on matters of security, including security risk management, the Technical Security Branch (TSB), of the Royal Canadian Mounted Police, is a very useful source.

7 APPLICATION

This policy guideline is effective as of April 1, 2003.

For persons registered prior to the effective date of this policy with a security plan considered appropriate in light of the previous guideline, they will need to comply with this policy guideline for renewal of their registration.

The security plan in place at the registered person's place of business is subject to being made available upon inspection by the CGD at any time over the period of registration.

This policy guideline will be reviewed periodically to assess its comprehensiveness.

The registered person should review the security plan periodically to ensure it continues to meet the security needs for safeguarding controlled goods and/or controlled technology.

8 ENQUIRIES AND COMMENTS

For enquiries, the CGD can be reached toll free at 1-866-333-2477 or by electronic mail: ncr.cgd@pwgsc.gc.ca. By mail, see the address at section 6 above.

The CGD's Internet site is: www.cgd.gc.ca.

Any comments on this policy guideline are welcome and can be forwarded to the Policy Manager, Controlled Goods Directorate.

APPENDIX

Legislative Text

Defence Production Act:

Section 40. Every registered person shall provide the Minister with any information prescribed by regulation, in the manner and time prescribed by regulation.

Controlled Goods Regulations:

Section 10. Every registration of a person is subject to the following conditions:

(e) that the person establish and implement a security plan in respect of each place of business in Canada where controlled goods are kept that contains written measures that set out

i. The procedures used by the person to control the examination, possession and transfer of controlled goods and/or controlled technology.
ii. The procedures for reporting and investigating security breaches in relation to controlled goods and/or controlled technology.
iii. The description of the responsibilities of the person's security organization and the identity of individuals who are responsible for the security of controlled goods and/or controlled technology, and
iv. The contents of security briefings and training programs given to visitors, officers, directors, employees and temporary workers, as the case may be;

(h) that the person advise the Minister, without delay, of any security breaches in relations to controlled goods and/or controlled technology;