The Development Process of a Security Plan

The purpose of the Security Plan
is to ensure that adequate security measures
are implemented
in the protection of controlled goods.

The Development Process of a Security Plan

The purpose of this document is to provide guidance in establishing a security plan related to the Controlled Goods Directorate (CGD). By no means should this document be used as a template, as security requirements differ from one company to another, and are determined by controlled goods being handled by the company. The security requirements of your company should be assessed on their own merits with respect to the requirements outlined in the *Defence Production Act* (DPA) and the *Controlled Goods Regulations* (CGR). For additional information on preparing a security plan, please refer to the Policy Guideline on Security Plans or contact our Call Centre (1-866-368-4646).

Note:

For the purpose of this document, person refers to an individual, a partnership or other business enterprises.

Step 1: Develop a plan

Person(s) with controlled goods on their premises must have a detailed security plan for each site where controlled goods are kept.

Person's Name and Site Address

SECURITY ORGANIZATION

The following people, on behalf of the person, will be responsible for the security of controlled goods and/or controlled technology at **(***Insert Person's Name*):

Mr./Ms. (*Insert Name*) is the Authorized Individual.

Mr./Ms. (*Insert Name*) is the Designated Official.

- (List Name and title of individuals who, on behalf of the person, will be managing controlled goods)

Responsibilities of the Security Organization

The responsibilities of the individuals stipulated above are as follows:

- The Authorized Individual, on behalf of the person, will be responsible for the following:

  - Ensure that a designated official is appointed for each place of business in Canada where controlled goods and/or controlled technology are kept; and

  - Approve by his/her signature any changes in any of the information contained in the application for registration.

- The Designated Official, on behalf of the person, will be responsible for the following:

  - With respect of each officer, director and employee who is not a temporary worker of the registered person who requires in the course of their duties access to controlled goods and/or controlled technology,

    - conducting, with the consent of the individual concerned, a security assessment in accordance with section 15 of the CGR;

    - determining, on the basis of a security assessment, the extent to which the individual concerned poses a risk for transferring controlled goods and/or controlled technology to any person who is not registered or exempt from registration;

    - making and keeping, on the basis of the security assessment, an evaluation as to the honesty, reliability and trustworthiness of the officer, director or employee concerned during the period of their employment and for a period of two years after the day on which they cease to be an officer, director or employee of the person;

    - authorizing, with respect to those individuals concerned who have been evaluated as being honest, reliable and trustworthy, the extent with which they may examine, possess or transfer controlled goods and/or controlled technology; and

  - submitting applications for exemptions to the Minister with respect to temporary workers or visitors.

- ❑ Mr./Ms. (*Insert Name of employee)* will be responsible, on behalf of the person, to keep and maintain, during the period of registration and for a period of five years after the day on which the person ceases to be registered, records that contain:

  - a description of any controlled goods and/or controlled technology received by the person, the date of their receipt and an identification of the person from whom they were transferred;

  - a description of any controlled goods and/or controlled technology transferred by the person, the date of their transfer and the identity and address of the person to whom they were transferred, and

  - a description of the manner and date of disposition of the controlled goods and/or controlled technology;

- ❑ Mr./Ms. (*Insert Name of employee)* will be responsible, on behalf of the person, to keep a copy of the evidence referred to in subsection 16(2) of the CGR for a period of two years after the day on which the individual who is exempt ceases to have access to the controlled goods and/or controlled technology of the registered person;

- ❑ Mr./Ms. (*Insert Name of employee)* will be responsible, on behalf of the person, to establish and implement a security plan with respect to each place of business in Canada where controlled goods and/or controlled technology are kept;

- ❑ Mr./Ms. (*Insert Name of employee)* will be responsible, on behalf of the person, to provide training with respect to the secure handling of controlled goods and/or controlled technology for officers, directors, employees and temporary workers who are authorized to possess or examine those goods;

- ❑ Mr./Ms. (*Insert Name of employee)* will be responsible, on behalf of the person, to provide briefings with respect to the secure handling of controlled goods and/or controlled technology by visitors who are authorized to examine those goods;

- ❑ Mr./Ms. (*Insert Name of employee)* will be responsible, on behalf of the person, to collect:

  - evidence of the individual's status as a director, an officer or an employee of the person registered to access controlled goods and/or controlled technology under the International Traffic in Arms Regulations, Title 22, Parts 120-130 of the Code of Federal

Regulations (United States) (Confirmation that the individual is employed by that person);

- evidence of the registration and eligibility of that person under the *International Traffic in Arms Regulations*;

- evidence of the eligibility of the individual under the *International Traffic in Arms Regulations*.

❑ Mr./Ms. (*Insert Name of employee)* will be responsible, on behalf of the person, to inform the Minister of any change of information contained in the application for registration.

❑ Mr./Ms. (*Insert Name of employee)* will be responsible, on behalf of the person, to (list any additional responsibilities you deem necessary)

PROCEDURES TO MONITOR THE CONTROLLED GOODS

Examination

Means to consider in detail or subject to an analysis in order to discover essential features or meaning.

In order to control the examination of controlled goods and/or controlled technology at (*Insert Person's Name*), the following procedures are to be followed:

❑ (*Insert list of procedures* to be followed by all employees)

Possession

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.

In order to control the possession of controlled goods and/or controlled technology at (*Insert Person's Name*), the following procedures are to be followed:

❑ (*Insert list of procedures* to be followed by all employees)

Transfer

> Means, with respect to a controlled good, to dispose of it or disclose its content in any manner.

In order to control the transfer of controlled goods and/or controlled technology at (*Insert Person's Name*), the following procedures are to be followed:

- (*Insert list of procedures* to be followed by all employees)

Note: Officers, directors, employees, and temporary workers need to be reminded of the importance not to discuss controlled goods matters with employees or other individuals who have not been the subject of a security assessment, as the discussion is considered a transfer of information.

BREACHES

Investigating and Reporting

Security breaches can be categorized as follows: loss, unauthorized examination/possession/transfer, willful damage, tampering of controlled goods and/or controlled technology. As a condition of registration under the CG Regulations (*Insert Person's Name*) must:

- report the security breach to the local police, if it is criminal in nature;
- advise the CGD, without delay, of any security breach in relation to controlled goods and/or controlled technology;
- the following investigative steps will be initiated: in order to identify the cause and to prevent reoccurrence (*Insert* the list of all the steps the Person will initiate in order to identify Who was involved? What Controlled Goods were involved? Where did the breach take place? When did the breach occur? Why did it occur? How did it occur? to rectify the situation in order to prevent reoccurrence of the breach);
- Document the security breach; and
- Implement corrective measures to ensure similar security breaches do not occur in the future.

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

- 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

Immediate notification of a security breach to the CGD allows for tracking and follow-up.

TRAINING PROGRAM

In order to maintain the Person's awareness of controlled goods and/or controlled technology, the officers, directors, employees and temporary workers will have to undergo the following training:

- Read the security plan on an annual basis;
- Read the CGD Newsletters; and
- (*Insert the list of any additional training* that would be pertinent to the Person, i.e., orientation training).

SECURITY BRIEFINGS

Visitors who have not received registration exemption from CGD will be informed that they will not be allowed to examine, possess, or transfer controlled goods in the course of their visit.

Visitors who have received registration exemption from CGD will be reminded through (*Please identify the means of communication used by the Person and list Person's security issues, i.e. confidentiality clause)*.

Step 2: Responsibility of the plan

It is the responsibility of the Person to establish and implement the Security Plan.

Step 3: Reviewing and approval

Although the Person delegated the task for developing the Security Plan, it remains the Person's responsibility.

Step 4: Implementation

Establish target dates and put the plan into action. Make security both proactive and reactive. Officers, directors, employees, temporary workers and visitors

should only examine, possess, or transfer controlled goods when necessary to perform their duties.

Step 5: Monitoring

Monitor the progress in implementing and reassessing the plan as needed. Look for opportunities to improve your plan and securities, especially as you upgrade your systems and software and expand the capabilities of your local area network and/or your data risk change. The process is never ending and you need to continually reassess your situation as the internal and external environment changes.

It is extremely important that you work closely with your technical staff and provide guidance to them, when necessary, to ensure the completion of your security plan.

P103-4/2008E-PDF
978-0-662-47720-4