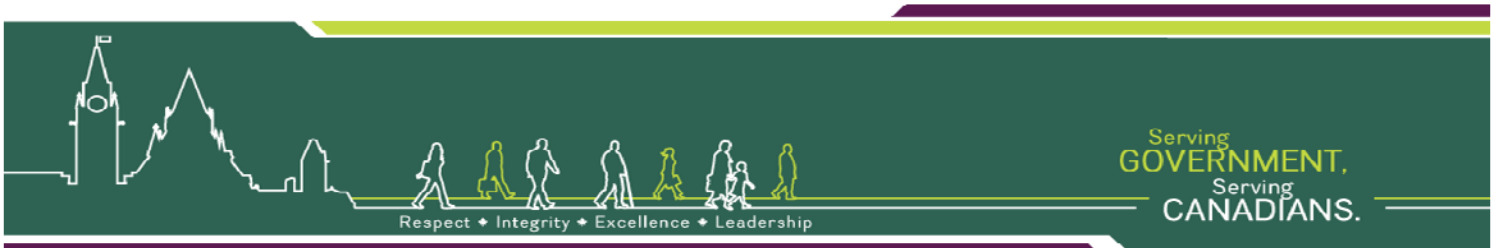

Developing a Security Plan

January 2013

Developing a Security Plan

The purpose of this document is to provide guidance in establishing a security plan related to the Controlled Goods Program (CGP) and to ensure that adequate security measures are implemented in the protection of controlled goods. This document should not be used as a template, as security requirements differ from one company to another and are determined by the type of 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 please refer to section 2.5 of the Guideline on CGP Registration or contact our Client Service Centre at 613-948-4176 or 1-866-368-4646 (toll free).

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 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 for each place of business in Canada where the person keeps controlled goods and/or controlled technology;
- 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 that the person deems necessary)

PROCEDURES TO MONITOR THE CONTROLLED GOODS

A BRIEF STATEMENT OUTLINING THE COMPANY's INVOLVEMENT WITH CONTROLLED GOODS (ie. XYZ Company manufactures made-to-order components for final use on light-armoured vehicles under contract to ABC Canada Inc.)

Examine

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

Possess

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.

Transfer

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

In order to control the EXAMINATION, POSSESSION and/or TRANSFER of controlled goods and/or controlled technology at (*insert person's name*), the following procedures have been implemented:

- Explain the company's procedures for handling controlled goods from the time a controlled good is first received, while in possession of the company (including the design and production process if applicable), until its final disposition (transfer or disposal). This would include controlled goods in all formats including, but not limited to: electronic data, technical schematics and physical goods. This should also include details of securing the goods while in the company's possession. Bullet format is preferable.

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.

Information Technology (IT) - REMOTE ACCESS

Remote access

Refers to communication with a data processing facility or server from a remote location through a data link. One of the more common methods of providing this type of remote access is using a Virtual Private Network (VPN).

In order to control and protect controlled goods information, a minimum standard of IT security must be exercised. The most accepted practices involve the use of a Wide Area Network (WAN) dedicated to the company or a VPN, which allows secure access to corporate resources by establishing an encrypted tunnel across the Internet.

If a company permits remote access to controlled goods information by its personnel or another entity, which is registered/exempt from registration with the CGP, it should consider the following:

- requests for remote access should be reviewed by the Designated Official (or his delegate) prior to approval.
- remote access should only be granted when required.
- Standard Operating Procedures detailing the security practices required by those persons granted remote access should be provided.

- the company must employ an acceptable form of IT security/encryption (VPN, WAN, etc.) in order to minimize the risk of unauthorized transfer of controlled goods information.

In order to minimize the risk of unauthorized examination, possession or transfer of controlled goods or controlled goods technology via remote access at *(insert person's name)*, the following procedures are to be followed:

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

BREACHES

Investigating and Reporting

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

- report the security breach to the local police, if it is criminal in nature;
- notify the CGP, without delay, of any security breach in relation to controlled goods and/or controlled technology;
- determine the answers to the following questions and initiate these steps (modify as required or add steps as deemed necessary) to identify the cause and prevent reoccurrence:
  - 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?
  - Document the security breach; and

- Implement corrective measures to ensure similar security breaches do not occur in the future.

The CGP is to be notified of a security breach via:

Telephone: 613-948-4176 or 1-866-368-4646 (toll free)
Facsimile: 613-948-1722
E-mail: dmc-cgd@tpsgc-pwgsc.gc.ca

Mailing Address

Controlled Goods Program
Public Works and Government Services Canada
2745 Iris Street, 3rd Floor
Ottawa ON K1A 0S5

Courier Address

Controlled Goods Program
2745 Iris Street, 3rd Floor
c/o PWGSC Central Mail Room
Place du Portage, Phase III, 0B3
11 Laurier Street
Gatineau QC K1A 0S5

Immediate notification of a security breach to the CGP allows for prompt 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 CGP 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 the CGP 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 the CGP 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

Even if the person delegated the task for developing the Security Plan, it still 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 it is necessary in order to perform their duties.

Step 5: Monitoring

Monitor the progress in implementing and reassessing the plan as needed. Look for opportunities to improve the plan and securities, especially if upgrading systems and software and expanding the capabilities of the local area network and/or the data risk changes. The process is ongoing and the person needs to continually reassess the situation as the internal and external environment changes.

It is extremely important that the person works closely with technical staff and provides guidance to them, when necessary, to ensure the completion of the Security Plan.