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

CONTROLLED GOODS DIRECTORATE

POLICY GUIDELINE - SECURITY ASSESSMENTS BY DESIGNATED OFFICIALS (OF REGISTERED PERSON)

Canada

TABLE OF CONTENTS

1. INTRODUCTION

As conditions of registration under the Controlled Goods Directorate (CGD), a registered person must appoint a designated official (DO) and ensure that the appointed DO conducts a security assessment of each officer, director and employee who require, in the course of their duties, access (examination, possession or transfer) to controlled goods and/or controlled technology.

The DO selected by the registered person should be someone with sufficient authority, responsibility and integrity within the business or company to adequately conduct such security assessments (e.g. security officer or human resources officer). This will be the subject of a future policy guideline.

DOs also conduct a preliminary security evaluation of a foreign temporary worker when an application is made by the registered person on behalf of such worker who will be accessing controlled goods and/or controlled technology. (This will be the subject of a future policy guideline - note that following the preliminary security evaluation by the DO, a CGD officer conducts the security assessment of the foreign temporary worker upon receipt of the application for exemption.)

2. OBJECTIVE

To provide policy guidelines for designated officials conducting security assessments of employees, directors and officers of the registered person (company) who will access controlled goods and/or controlled technology at the registered person's place of business.

3. LEGISLATIVE POLICY

Every registered person must ensure that the DO carries out security assessments in the following manner.

In regard to each officer, director and employee of the registered person who in the course of their duties have access to controlled goods and/or controlled technology, the DO is required to:

- conduct, with the consent of the individual concerned, a security assessment in accordance with regulatory criteria noted below.
- determine, on the basis of the security assessment, the extent to which the individual concerned poses a risk of transferring controlled goods and/or controlled technology to any person who is not registered or exempt from registration.

- make and keep, on the basis of the security assessment, an evaluation as to the honesty, reliability and trustworthiness of the individual concerned.
- authorize, in respect of those individuals concerned who have been evaluated as being honest, reliable and trustworthy, the extent to which they may examine, possess or transfer controlled goods and/or controlled technology.

The registration of a person extends to each officer, director and employee of the registered person authorized by the designated official to access controlled goods and/or controlled technology, but only when the individual acts in the course of their duties with the registered person. No registered person, including such person by extension, shall knowingly transfer a controlled good or permit the examination of a controlled good by a person who is not registered or exempt from registration.

Regulatory Criteria - For the purpose of determining the honesty, reliability and trustworthiness of a person and the extent to which the person poses a risk of transferring a controlled good to a person who is not registered or exempt from registration, the DO must conduct a security assessment that takes into account the following over the five years prior to the persons' consent to such assessment:

- personal references
- criminal history
- place(s) of residence
- employment history
- educational history

The individual, subject to the security assessment, must provide the DO their date of birth and evidence of personal references, criminal history, place(s) of residence and employment and educational history. This evidence must be capable of being verified by the CGD.

The individual, subject to the security assessment, must provide without delay information regarding any change concerning criminal history. Upon receipt of such information, the DO must reconduct a security assessment.

If there are reasonable grounds, the DO may reconduct a security assessment for the purpose of determining the extent to which the person poses a risk of transferring a controlled good to a person who is not registered or exempt from registration.

References: Sections 13, 14 and 15 the Controlled Goods Regulations and subsections 37(2) and paragraph 43(b) of the Defence Production Act

For guidelines on these legislative references, see section 6 f this Policy Guideline.

4. POLICY RATIONALE

DOs, as on-site representatives of the registered person, are well positioned to evaluate each employee, director and officer of the registered person, having access to controlled goods and/or controlled technology, in terms of their honesty, reliability and trustworthiness and the extent to which each poses a risk of transferring a controlled good to an unauthorized person. Security assessments contribute to the safeguarding of controlled goods and/or controlled technology by employees, directors and officers of registered persons, thus preventing such goods from falling into unauthorized hands. There are stringent penalties for those who knowingly violate the DPA.

5. DEFINITIONS

Designated official (DO), means an employee of the registered person who has been appointed by the registered person, subject to approval upon a security assessment by the CGD, to carry out certain duties such as to conduct a security assessment of each officer, director and employee of the registered person (except temporary workers) who requires in the course of their duties access to controlled goods and/or controlled technology. The DO must be either a Canadian citizen ordinarily resident in Canada or a permanent resident ordinarily resident in Canada.

Registered person, means an individual, corporation, partnership or any other business enterprise, registered under the CGD.

Officer, means the chairperson or vice-chairperson of the board of directors, the president, any vice-president, the secretary, any assistant secretary, the treasurer, any assistant treasurer, the general manager and any other person designated an officer by by-law or by resolution of the directors, and any other individual who performs functions for the company similar to those normally performed by an individual occupying any of those offices.

Director, means a person who manages the affairs and business of the company.

Employee, means a person employed by the registered person to perform duties for remuneration under either a contract of or for services.

Agent, means one who is authorized to act for or in place of another; a representative.

Honesty, the quality of being honest - fair and just in character of behavior - not cheating or stealing - free of deceit, untruthfulness and misrepresentation - sincere.

Reliability, reliable; suitable or fit to be relied on; of sound and consistent character or quality. Reliable suggests that the person it describes can safely be believed or trusted and counted on to do or be what is expected, wanted or needed.

Trustworthy, fully deserving of complete confidence in one's truthfulness, honesty, good judgment, justice, etc.; the obligation or responsibility imposed on a person in whom confidence or authority is placed; the condition of one in whom trust has been placed; being relied on.

Controlled goods, as listed in the schedule to the DPA, are those military, strategic and military-related goods and technology, as well as dual-use goods and technology as identified in Group 2 (not all items), item 5504 and Group 6 (all items), of the Export Control List (ECL) made under authority of the Export and Import Permits Act (EIPA) and 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. See the Schedule to the DPA.

The Export Control List is at the ITC 's internet site:
www.dfait-maeci.gc.ca/~eicb/export/contente.htm

6. POLICY GUIDELINES ON CONDUCTING SECURITY ASSESSMENTS

6.1 Consent to a Security Assessment

Each employee, director and officer of the registered person who has access to controlled goods and/or controlled technology during the course of their employment must consent to a security assessment. No security assessment is required if the employee, director or officer does not access controlled goods and/or controlled technology.

If the employee, director or officer does not consent, they cannot have access to controlled goods and/or controlled technology.

Consent would be normally provided by the employee, director or officer by completing the "Security Assessment Application - Employee, Director, Officer" (Appendix 1). An information sheet has been developed which the DO can provide to the employee, director or officer, which explains the requirement for a security assessment (Appendix 2).

6.2 Consent To Use a Government of Canada Security Clearance

If an officer, employee or director subject to a security assessment under the Controlled Goods Directorate has a valid security clearance granted by the Government of Canada (GOC) at the Secret level or higher, this is considered sufficient for the purpose of a security assessment under the CGD. Consequently, the Designated Official will not have to conduct a CGD security assessment on these individuals.

See appendix 3 for a consent form to be completed by the employee, director or officer who has been granted a GOC clearance at the Secret level or higher. A signed copy of the consent form must be kept in the registered person's record keeping system. Note from the consent form that the information to be released as part of the consent can only be utilized for the purpose of a security assessment under section 15 of the Controlled Goods Regulations. It is important that the individual providing the consent understand that the information consented to be released will be fully protected under the *Defence Production Act*, the *Privacy Act* and the *Personal Information Protection and Electronics Documents Act*.

A GOC security clearance is only acceptable under CGD for the period of its validity. If a GOC security clearance expires and is not immediately renewed the designated official will now have to conduct a CGD security assessment on the individual in question.

Si un employé, le cadre ou l'administrateur assujetti à une évaluation de sécurité en vertu de la Direction des marchandises contrôlées possède une cote de sécurité valide de niveau secret ou de niveau supérieur accordée par le gouvernement du Canada, cette cote de sécurité est acceptable pour l'évaluation de sécurité dans le cadre de la DMC. Par conséquent, le représentant désigné n'a pas à procéder à une nouvelle évaluation de sécurité de la DMC sur les personnes susmentionnées.

6.3 General

Once the application has been completed by the employee, officer or director of the company, the DO reviews the application to ensure all the information requested has been provided. If there is missing information, the DO obtains the missing information from the applicant.

The DO must ensure that the applicant has provided all the necessary information as to personal references, criminal history, places of residence and employment and educational histories for the five years immediately preceding the date of the applicant's consent to undergo the security assessment.

The DO then verifies the information by utilizing the "Verification Document for Designated Official Conducting a Security Assessment of an Employee, Director, Officer" (Appendix 4) in regard to the information required to be provided by the applicant:

- Personal references
- Criminal history
- Places of residence
- Employment and educational histories

Sample questions for follow-up by the DO are available in Appendix 5.

6.4 Personal References

Based on circumstances, the DO could decide to contact two individuals identified as personal references, preferably the individuals who appear the most knowledgeable of the person being assessed. Contact with those two references would allow for a basis of comparison.

Checking personal references assists in determining whether the person being assessed has been honest, reliable and trustworthy. It is important to check personal references going back the last five years.

A list of sample questions is provided to assist the DO when contacting personal references (Appendix 5). Should the DO need to clarify the information obtained, other references or persons are to be contacted.

6.5 Criminal History

There are very limited circumstances where if an applicant has answered "no" to question 16 (see Appendix 1) in regard to criminal convictions, there would be no need to do any further verification. Obviously, the DO, based on other information in the application, may consider it appropriate to do so. (By example, new employees who are not well known to the company by the DO compared to employees of longer standing with the company) If the DO considers that further verification is needed, an appropriate avenue is to request a criminal record name check (CRNC). A CRNC can be obtained from the local police force either by the DO or by the individual subject to being security assessed (there is usually a fee for a CRNC).

If the CRNC reveals no criminal history, there is no need to do any further verification unless the DO, based on other information in the application, considers it appropriate to do so. If so, the DO may request the individual being security assessed to undergo a fingerprints check.

An affirmative answer to question 16 does not by itself put into question the applicant's honesty, reliability and trustworthiness and whether the applicant poses a risk of transferring a controlled good to an unauthorized person. The additional information provided by the applicant in relation to the criminal conviction and the nature of the conviction needs to be considered. For example, an isolated conviction for impaired driving is not by itself indicative of dishonesty, unreliability or untrustworthiness.

On the other hand, for example, a conviction for auto theft is indicative of the need to question further both the personal references and the individual subject to the security assessment application as such conviction raises a serious element of doubt as to the individual's honesty, reliability and trustworthiness.

A criminal record should be considered in light of such matters as the duties to be performed, the nature and frequency of the offence, the passage of time and the relationship to the registered person' s business.

A criminal act for which a pardon has been granted is not to be taken into account for criminal history.

Criminal history for only the last five years is required to be examined. The regulations do not require such history for the period prior to the last five years.

6.6 Places of Residence

Residence at one place over a long period of time is an indication of stability and reliability. On the other hand, several places of residence over the last five years are not by itself indicative of instability or unreliability. The listing of several places of residence may only be indicative of employment change or moving into larger accommodation as the family grows or matures.

Several moves particularly in the last year or so should be questioned further by the DO.

Neither is residence outside the country in the last five years indicative by itself of any personal instability or unreliability. The applicant may be a newly arrived immigrant with permanent residency or a newly accepted citizen of Canada. The applicant may also have been a continuous employee of the same firm simply moving to new work locations at the employer's request.

Past residence in another country that is not part of a list of countries that are considered like-minded should be questioned by the DO; this is to ensure that that there is no influence over the individual being assessed by a country unfriendly to Canadian interests.

If the DO has concerns from the information provided regarding residence in foreign countries in the last five years, the DO could request the individual under assessment to obtain a fingerprints imprint from the local police authority or an accredited fingerprints agency. This in turn can be forwarded to the CGD, which would have the fingerprints imprint of the individual checked out against international records.

6.7 Employment and Educational Histories

Employment history assists in determining reliability in the current and previous employment and along with educational qualifications, assists in determining whether the person is being truthful about background and employment and qualifications history.

Long-term employment with the same employer can be indicative of loyalty, dedication and commitment. Frequent changes in employment may be nothing more than the result of a progressive career path or moving to accompany a relocated spouse. Frequent changes in employment should be questioned further by the DO to ensure that such does not put the applicant's honesty, reliability and trustworthiness in doubt.

Personal education completed years ago combined with long-term attachment to the same employer is indicative of stability and reliability. Recent and progressive educational accreditations could be indicative of initiative, productiveness and increasing self-worth, all supportive indicators of personal reliability.

A recent history of frequent movement from one educational institution to another should be questioned further by the DO to ensure that such does not put the applicant's honesty, reliability and trustworthiness in doubt.

6.8 Consultation with the Registered Person's Human Resources Section

DOs should not consider themselves working in isolation. They can and should consult with the company's Human Resources (HR) section for additional personal information or verification relative to determining the individual' reliability, honesty and trustworthiness. The company's HR practitioner can be a good supporting source in regard to confirming information on personal references, criminal history, employment history and educational qualifications, over the last five years.

In some instances, the HR practitioner and the DO may be one and the same.

The "Consent" form (see Appendix 1), to be completed by the individual to be assessed, requests the individual to not only provide consent to undergo a security assessment but also to allow access to any personal information on the individual's HR file which would be useful in assisting the security assessment to be conducted by the DO.

6.9 Assessment Guideline

An interview with the applicant is suggested where there appears to be conflicting information. Such interview would assist the DO in clarifying the information and/or assessing the credibility of the applicant.

All of the information obtained by the DO needs to be evaluated. The evaluation process is in the nature of an administrative judgment, i.e. the facts are weighed and the decision to be made rests on which side the scale tips. For example, if the facts weigh out on the side of the employee, director or officer being reliable, trustworthy and honest, then a determination to that effect would be appropriate. If the facts on each side of the issue are equally balanced, as a principle of administrative law, the benefit of the doubt should be resolved in favour of considering the employee, director or officer as reliable, trustworthy and honest.

In cases where the credibility of an employee, director or officer is at play, the DO is well placed, particularly in an interview setting, to assess the person's credibility.

6.10 Extent of Posing a Risk of Unauthorized Transfer

In addition to reliability, honesty and trustworthiness, the DO is required to assess the extent to which the employee, director or officer poses a risk of transferring a controlled good to an unauthorized person. Once the judgment has been made by the DO that the person is honest, reliable and trustworthy, it follows that the person would not pose a risk of transferring a controlled good to an unauthorized person.

6.11 Authorization of Extent to Examine, Possess or Transfer

Upon a judgment to the effect that the individual concerned is honest, reliable and trustworthy, the DO is required to authorize the extent to which the individual (officer, director or employee) may examine, possess or transfer controlled goods and/or controlled technology.

What is meant by "extent" above? In its context, it means something apart from honesty, reliability and trustworthiness. It relates more to the level of responsibility the DO should recognize for the employee, director or officer in accessing (examining, possessing and transferring) the company's controlled goods and/or controlled technology. It also relates to the nature of the controlled goods and/or controlled technology and the degree of security required to safeguard those controlled goods and/or controlled technology.

As mentioned earlier, the DO selected by the registered person should be someone with sufficient authority, responsibility and integrity within the business or company to adequately conduct security assessments. As further mentioned, DOs, as on-site representatives of the registered person, are well positioned to evaluate each employee, director and officer of the registered person having access to controlled goods and/or controlled technology.

Therefore, each DO is in the unique position of understanding the nature of the registered person's business and controlled goods and/or controlled technology and responsibility level to be accorded to each employee, director and officer accessing controlled goods and/or controlled technology.

For example, a senior engineer with a company that produces ammunition and components specially designed for controlled goods and/or controlled technology could be considered by the DO to have full extent (or access) to examine, possess and transfer controlled goods and/or controlled technology, whereas an employee whose duties consist mainly of moving controlled goods and/or controlled technology within a warehouse could be considered for partial extent (such as handling only - no detailed examination or exploration). Finally, despite the situation, the security evaluation process is the same for every applicant, regardless of whether they will be granted full extent/access or only partial extent/access to controlled goods and/or controlled technology.

6.12 Negative Evaluation

When a DO determines that the employee, officer or director is not reliable, honest and trustworthy and that such individual poses a risk of transferring a controlled good to an unauthorized person, such individual cannot be allowed to access controlled goods and/or controlled technology at the employer's (registered person) place of business. See Appendix 7 for information that should be provided to the individual.

Should the person affected by such a negative evaluation contest such evaluation, the person should be allowed to provide any additional information that could affect the evaluation. See section 6.13 for the possibility of reconducting a security assessment. Furthermore, as part of a supportive approach, the DO could consult a CGD registration officer to have their input in specific cases given their own experience of performing background references on DOs.

6.13 Reconducting a Security Assessment

Pursuant to section 15 of the CGR, the DO shall reconduct a security assessment after receiving information regarding any change in criminal history.

The DO may, if there are reasonable grounds for doing so, reconduct a security assessment for the purpose of determining the extent to which the employee, director or officer poses a risk of transferring a controlled good to an unauthorized person. A reasonable ground in the case of a "negative evaluation" may be new information supportive of a person's reliability, trustworthiness and honesty.

6.14 Duration of Positive Security Assessment Evaluation

Once the DO has evaluated the employee, officer or director and determined that such person is honest, reliable and trustworthy and does not pose a risk of transferring a controlled good to an unauthorized person, such evaluation can be accepted for up to ten years, as long as the person remains in the employ of the same registered person. The evaluation can be revised at any time prior to the 10 year period should the DO consider is appropriate to do so in view of particular circumstances.

The employee, director or officer who has been positively security assessed is to be informed by the attached, "Information Note to Employee, Director or Officer on Being Security Assessed" (Appendix 6).

6.15 Scope of Registration

Once the DO has conducted a security assessment on the employee, officer or director and authorized the extent to which such person can examine, possess or transfer controlled goods and/or controlled technology, the registration of the employing company extends to each officer, director or employee so authorized by the DO. Such extension of registration only applies when the individual acts in the course of their duties with the registered person.

Once security assessed therefore, the employee, director or officer is placed at a high level of responsibility in regard to safeguarding controlled goods and/or controlled technology at the registered person's place of business. They become subject to the requirements of subsection 37(2) of the DPA, i.e. they would be in an offence situation under the DPA if they knowingly transfer controlled goods and/or controlled technology to an unauthorized person or permit the examination of controlled goods and/or controlled technology by an unauthorized person. Offences under section 37 of the DPA could be brought to prosecution with penalties up to $ 2 million for each offence, a prison term of ten years, or both.

6.16 Liability of Officer, Director or Agent of a Corporation

Whether subject to a security assessment or not, there is section 46 of the DPA which subjects an officer, director or agent of a corporation to liability under the DPA when their corporation commits an offence under the DPA. The officer, director or agent is liable to be convicted of the offence if they directed, authorized or assented to, acquiesced in or participated in the commission of the offence, whether or not the corporation has been prosecuted or convicted.

7. APPLICATION

This policy guideline is effective as of September 8, 2003.

For persons security assessed by a DO prior to the effective date of this policy, the security assessment will be valid for no longer than five years from the date of the original security assessment evaluation. A DO can nevertheless reconduct a security assessment as per section 6.13 of this policy guideline.

The security assessments conducted by the DO at the registered person's place of business are subject to being made available upon inspection by the CGD at any time over the period of registration and for a period of two years after the day on which the person ceases to be an employee, officer or director of the registered person.

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

8. ENQUIRIES AND COMMENTS

To obtain additional information, visit the CGD web site at: **www.cgd.gc.ca**

For enquiries, the CGD can be reached toll free at 1-866-368-4646 or by electronic mail: ncr.cgd@pwgsc.gc.ca.

By mail, the address is:
Controlled Goods Directorate of Canada
Public Works and Government Services Canada
C/O Central Mail Room
Place du Portage, Phase III OB3
11 Laurier Street, Gatineau
K1A 0S5

Physical location is:
3rd Floor
2745 Iris Street
Ottawa, Ontario

Any comments on this policy guideline are welcome and can be forwarded to the address above or by electronic mail: **Attention: Manager Policy, Controlled Goods Directorate.**

ANNEXE 1 – "SECURITY ASSESSMENT APPLICATION" - EMPLOYEE, DIRECTOR, OFFICER

This application form is not for temporary workers (who are not either a Canadian citizen or a permanent resident ordinarily residing in Canada). For these, one needs to complete a separate application for exemption from registration.

A - Consent to a security assessment:

I understand the need for a security assessment since in the course of my duties I will examine, possess and/or transfer controlled goods. I give my consent to the Designated Official of the registered person (Company's name)

_____

to conduct a security assessment using the personal information provided in the questionnaire below and any information in the human resources file the company keeps on me.

_____ Signature	_____ Date (YYYY-MM-DD)

WITH YOUR CONSENT, PLEASE COMPLETE THE FOLLOWING QUESTIONNAIRE

B - General Information

1. Surname (last name)	2. Full given name(s) (no intial), underline usual name used
3. All other names used (i.e. former name, maiden name or nicknames)	4. Date of birth (YY-MM-DD)
5. Business title	6. Business civic address (street address)
7. Business telephone no.	8. Home telephone no.
9. Business facsimile no.	10. Business e-mail address

11. Are you a Canadian citizen or permanent resident of Canada?	12. Attach a copy of one of the following:
☐ YES ☐ NO (please explain)	• Valid Canadian Driver's License • Provincial Health Card • Employee Identification Card • Passport • Canadian "Citizenship Certificate" • Canadian "Birth Certificate" (or "Baptismal Certificate") • "Record of landing" (IMM1000)

C – Addresses

List your address(es) for the past 5 years, beginning with the most recent (use extra sheet if necessary)

Street address, City, Province/State, Postal/Zip code, and Country	From (YY-MM)	To (YY-MM)
13a.		
b.		
c.		
d.		
e.		

D - Activities

Activities during the past 5 years, beginning with the most recent (use an extra sheet if necessary). Account for the entire period, including employment, unemployment, education, etc. If applicable, attach evidence of your educational history (such as a copy of your diploma or degree).

Activity	Street address, city, province/state, postal/zip code and countrys	From (YY-MM)	To (YY-MM)
14a.			
b.			
c.			

d.			
e.			

E - Personal References

Provide 3 personal references whose combined knowledge of you covers the past 5 years (relatives are not suitable references)

Name	Residential address	Home telephone no.	Business telephone no.
15a.			
b.			
c.			

F - Criminal History

16. Have you ever been convicted of a criminal offence in or outside of Canada for which you have not been granted a pardon? (The existence of such a record, provided it is declared, may not be an impediment to having access to controlled goods and each case will be judged on its own merit.)

- ☐ Yes
- ☐ No

If you have replied yes to number 16, you must provide the following details :

a. Description of the charges	
b. Name of police force	c. City, Province/State and Country
d. Date of conviction (YY-MM-DD)	e. Surname (last name) at the time of the conviction

G - Modification

Vous devez signaler sans délai tout changement concernant les renseignements fournis dans la section F.

H – Declaration

I certify that the information contained in this application is true, complete and correct, and acknowledge and agree to comply with the responsibilities outlined in the *Defence Production Act*. Specifically, I recognize the need as per section 37 to ensure that only authorized persons are allowed to examine or possess controlled goods and that controlled goods are transferred only to authorized persons. I understand that there could be severe sanctions under section 45 for offences under section 37. I also understand that there could be stringent penalties under sections 44 and 45 for any false or misleading statements..

Signature	Date (YYYY-MM-DD)

APPENDIX 2 - INFORMATION SHEET FOR THE EMPLOYEE, DIRECTOR AND OFFICER SUBJECT TO A SECURITY ASSESSMENT UNDER THE CONTROLLED GOODS DIRECTORATE

Objective of the program

The objective of the CGD is to safeguard controlled goods and/or controlled technology within Canada and prevent controlled goods and/or controlled technology from falling into unauthorized hands. This is done by regulating the access, possession and transfer in Canada of certain goods.

Consent to provide personal information

Under the Controlled Goods Regulations (CGR), each employee, director and officer who require in the course of their duties access to controlled goods and/or controlled technology need to give their consent permitting the Designated Official (DO) to conduct a security assessment. You are asked to complete the "Security Assessment Application" and ensure that it contains all the required information. Once completed, it is your responsibility as required by the CGR to report promptly to your DO any changes to the information you provided in regard to criminal activity.

Personal information you provide in this application is collected under the authority of the *Defence Production Act* (DPA) and should be capable of being verified by the DO for the purpose of the security assessment or by the CGD when necessary.

Under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*, personal information you provide shall be protected by security safeguards appropriate to the sensitivity of the information..

Accountability

Under the DPA and the CGR, the registration of a person (Company) extends to each officer, director and employee of the registered person authorized by the DO to access controlled goods and/or controlled technology, when the individual acts in the course of their duties with the registered person.

The DPA carries penalties for making false or misleading statements, destroying records, making false record entries, interfering with the detainment action of a CGD inspector, failing to comply with any reasonable request of an inspector or obstructing the performance of an inspector's functions. The DPA carries heavier penalties for persons with access to controlled goods and/or controlled technology who knowingly allow an unauthorized person to examine a controlled good or transfer a controlled good to an unauthorized person (Sections 37, 44 and 45 of the DPA).

APPENDIX 3 - CONSENT TO USE A GOVERNMENT OF CANADA SECURITY CLEARANCE

Information provided in this consent form can only be used for the purpose of a security assessment under section 15 of the *Controlled Goods Regulations*.

A – Administrative Information		
1 - Surname	2 - Given name(s) (underline the usual name used)	
3 - Date of birth (YYYY-MM-DD)	4 - Business title	
5 - Legal name of registered business	6 - Business civic address	
7 - Business telephone number ( ) -	8 - Business facsimile number ( ) -	9 - Business e-mail address

B – Security Clearance Information

1 - Type of clearance (check one and attach evidence of the clearance)

☐ Secret ☐ NATO Secret

☐ Top Secret ☐ Other (specify) _____

2 - Issuing government organization

3 - Period of validity

_____ _____

Start date (YYYY-MM-DD) End date (YYYY-MM-DD)

C – Certification and Consent to Use a Government of Canada Security Clearance

I, the undersigned, do hereby certify that the information contained in this consent form is true, complete and correct. I understand the need for a security assessment, since in the course of my duties I will examine, possess or transfer controlled goods and/or controlled technology. I give my consent to the Controlled Goods Directorate/Designated Official of the above-mentioned registered business to use the security clearance that I obtained from the Government of Canada and any information relative to such clearance. I acknowledge and agree to comply with the responsibilities outlined in the *Defense Production Act* and the *Controlled Goods Regulations* with respect to examining, possessing and transferring controlled goods and/or controlled technology in Canada.

_____ _____

Signature Date (YYYY-MM-DD)

Protection of Information

Information provided in this consent form is protected and used in accordance with the provisions of the *Privacy Act*, the *Personal Information Protection and Electronic Documents Act* and the *Defence Production Act*.

APPENDIX 4 - VERIFICATION DOCUMENT FOR DESIGNATED OFFICIAL CONDUCTING A SECURITY ASSESSMENT OF AN EMPLOYEE, DIRECTOR, OFFICER

1. Registered Person 2. Name of the Designated Official	3. Employee, Director or Officer - Name 4. Title 5. Interview Date

Assessment Summary (Findings)

Recommendation & Conclusion (List the reasons for your decision)

Determination of Designated Official:

I, the undersigned,have reviewed the information provided by the person in question and based on an evaluation of this information and its verification, I have determined that this person (person's name),

_____

eis honest, reliable and trustworthy and does not pose a risk of transferring a controlled good to a person who is not registered or exempt from registration (as required by Sections 13 and15 of the *Controlled Goods Regulations*)

Signature	Title	Date (YYYY-MM-DD)

Ensure that the individual is thoroughly briefed concerning his responsibility. This briefing shall precede permission to access controlled goods.

Note:
The Assessment application needs to be verified. Personal references need to be taken into account (i.e. checked out).

- The DO should summarize in writing the reference information that was obtained, the name of the person, phone number and date of conversation.
- Always be prepared to probe further to clarify answers.
- For a period of residence outside Canada within the 5 years preceding the "Security Assessment Application" and when more information concerning security is necessary, the DO could communicate with CGD for assistance.

Requirement to Maintain Records

The registered person must keep and maintain records of security assessments and supporting documentation in respect of each officer, director or employee who possesses or transfers controlled goods, during the period of the employment and for a period of two years after the day on which they cease to be an officer, director or employee. Because a security assessment documentation contains personal information, it should not be retained in the organization personnel file, but rather in a separate and secure location, preferably with all the controlled goods records.

It is suggested that the registered person maintains a current listing of all employees, officers and directors who have been security assessed..

Personal Information

Under the *Privacy Act*:

7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for

a. the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or;
b. a purpose for which the information may be disclosed to the institution under subsection 8(2).

Under *Personal Information Protection and Electronic Documents Act*:

"An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party." [Section 4.1.3 (Schedule 1; Section 5)].

"Personal information shall be protected by security safeguards appropriate to the sensitivity of the information." [Section 4.7 (Schedule1; Section 5)].

Non-Disclosure of Information

Under the *Defence Production Act* (Section 30):

"No information with respect to an individual business that has been obtained under or by virtue of this Act shall be disclosed without the consent of the person carrying on that business, except:

a. *to a government department, or any person authorized by a government department, requiring the information for the purpose of the discharge of the functions of that department; or*
b. *for the purposes of any prosecution for an offence under this Act or, with the consent of the Minister, for the purposes of any civil suit or other proceeding at law."*

APPENDIX 5 - SAMPLE QUESTIONS FOR FOLLOW-UP BY THE DO

1) Regarding reference checks:

a. In what capacity have you known the subject? And for how long?
b. How well do you know the subject? (Personal- friends- social.)
c. Where do you know the subject from? (Employment, school, social acquaintance, etc.)
d. Confirm employers and addresses?
e. Confirm employment(s) and home addresses?
f. What was subject title and dates of employment with your organization?
g. Are you related through family to the subject? (If related, determine the relationship and immediate family).
h. Are there any additional comments you would like to add concerning the subject?

2) Do you feel that the subject is an honest, reliable and trustworthy person?

a. If yes, ask the reference/source for examples to confirm his/her opinion
b. If no, ensure examples are provided and use the "W5" method to solicit response (When, Where, Who, What, Why).
c. Do you consider the subject a conscientious and responsible person in ensuring that a company good or item requiring a high standard of security and secure handling is, not transferred to a person or company who had not been security assessed; and not allowed to be examined by a person who has not been security cleared?

3) Are you aware of any ongoing or recent criminal or civil litigation involving the subject? Describe them (when, where, who, what, why).

If these exist, how are they impacting on the subject's day-to-day life relative to the subject's honesty, reliability and trustworthiness?

4) re you aware of any trips/travel outside of Canada the subject is involved with? Frequency?

5) Do you know of any reason(s) that would impact on the subject suitability to possess, examine or transfer controlled goods?Please elaborate.

6) Are you aware of any associates or associations, which might be considered to have an adverse affect on the subject's position of trust?

APPENDIX 6 - INFORMATION NOTE TO EMPLOYEE, DIRECTOR OR OFFICER ON BEING SECURITY ASSESSED

Name of person security assessed :	
Name of registered person:	

This is to inform you that you have been security assessed under section 15 of the Controlled Goods Regulations. This means that you are authorized to examine, possess or transfer controlled goods while in the employ of: (Name of company)

Limitations on the extent of authorization:

(To DO: insert additional note regarding any limitations on the extent of authorization)

It is important that you are aware of what this security assessment means. For the purpose of the Defence Production Act and the Controlled Goods Regulations, the scope of your company's registration under the Controlled Goods Directorate extends to you when acting in the course of your duties with: (Name of company)

This means that if you knowingly transfer a controlled good to an unauthorized person or permit the examination of a controlled good by an unauthorized person, you may be subject to prosecution which carries a fine of up to $ 2 million for each offence, a jail term of 10 years, or both.

Authorized persons are other registered companies, persons exempted from registration by the CGD upon approved application (foreign temporary workers and visitors) and excluded persons (persons acting in good faith in the course of their duties while occupying a position in the federal public service or a federal Crown Corporation or employed by a province or territory of Canada).

It is also important that you inform the company of any change in information that may put your security assessment in doubt, such as involvement in criminal action.

Your security assessment is considered valid for a period of up to 10 years and is subject to revision at any time from the date of this information notice.

Name of Designated Official:

Signature	Date

Note:

Requirement to Maintain Records

The registered person must keep and maintain records of security assessments and supporting documentation in respect of each officer, director or employee who possesses or transfers controlled goods, during the period of the employment and for a period of two years after the day on which they cease to be an officer, director or employee. Because a security assessment documentation contains personal information, it should not be retained in the organization personnel file, but rather in a separate and secure location, preferably with all the controlled goods records.

It is suggested that the registered person maintains a current listing of all employees, officers and directors who have been security assessed.

Personal Information

Under the *Privacy Act*:

7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or

a. except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or
b. for a purpose for which the information may be disclosed to the institution under subsection 8(2).

Under *Personal Information Protection and Electronic Documents Act:*

''An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.'' [Section 4.1.3 (Schedule1; Section 5)].

"Personal information shall be protected by security safeguards appropriate to the sensitivity of the information." [Section 4.7 (Schedule1; Section 5)].

Non-Disclosure of Information

Under the *Defence Production Act* (Section 30):

"No information with respect to an individual business that has been obtained under or by virtue of this Act shall be disclosed without the consent of the person carrying on that business, except:

a. *to a government department, or any person authorized by a government department, requiring the information for the purpose of the discharge of the functions of that department; or;*

b. *for the purposes of any prosecution for an offence under this Act or, with the consent of the Minister, for the purposes of any civil suit or other proceeding at law."*

APPENDIX 7 - INFORMATION TO EMPLOYEE, DIRECTOR OR OFFICER ON BEING SECURITY ASSESSED (Negative Assessment)

Name of person security assessed :	
Name of registered person:	

This is to inform you that you have been evaluated under section 15 of the Controlled Goods Regulations. From all the information provided and obtained, it has been determined that you cannot be security assessed to access controlled goods. Section 15 requires that the information support a determination of honesty, reliability and trustworthiness and of non-risk of transferring a controlled good to an unauthorized person.

This means that you are not authorized to examine, posses or transfer controlled goods while in the employ of:

(Name of company)

If you disagree with this notice, you may request a review, providing any additional information that can assist such review.

Name of Designated Official:

_____ Signature	_____ Date

Note:

Requirement to Maintain Records

The registered person must keep and maintain records of security assessments and supporting documentation in respect of each officer, director or employee who possesses or transfers controlled goods, during the period of the employment and for a period of two years after the day on which they cease to be an officer, director or employee. Because a security assessment

documentation contains personal information, it should not be retained in the organization personnel file, but rather in a separate and secure location, preferably with all the controlled goods records.

It is suggested that the registered person maintains a current listing of all employees, officers and directors who have been security assessed.

Personal Information

Under the *Privacy Act*:

7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or

a. except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or
b. for a purpose for which the information may be disclosed to the institution under subsection 8(2).

Under *Personal Information Protection and Electronic Documents Act:*

''An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.'' [Section 4.1.3 (Schedule1; Section 5)].

"Personal information shall be protected by security safeguards appropriate to the sensitivity of the information." [Section 4.7 (Schedule1; Section 5)].

Non-Disclosure of Information

Under the *Defence Production Act* (Section 30):

"No information with respect to an individual business that has been obtained under or by virtue of this Act shall be disclosed without the consent of the person carrying on that business, except:

a. *to a government department, or any person authorized by a government department, requiring the information for the purpose of the discharge of the functions of that department; or;*

b. *for the purposes of any prosecution for an offence under this Act or, with the consent of the Minister, for the purposes of any civil suit or other proceeding at law."*