Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Security Organization and Administration Standard

Published: Jun 01, 1995

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-25/1995E-PDF
ISBN: 978-0-660-09998-9

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Norme de sécurité relative à l'organisation et l'administration

Security Organization and Administration Standard

1. Introduction

1.1 Purpose and scope

This document establishes the operational standard for the organization and administration of security as required by the Security policy. The standard contains both requirements, indicated by use of the word "must" in sentences appearing in italics, and recommended safeguards, indicated by use of the word "should."

1.2 Roles and responsibilities

Departments are responsible for protecting sensitive information and assets under their control in accordance with the Security policy and its operational standards.

The contracting authority is responsible for ensuring that the Security policy is complied with and that contract documentation includes the necessary clauses.

1.3 Concept

It can be useful to the management of the departmental security function to view security as a sub-system within the overall administrative and management system.

Inputs to the security system include:

- Policy support from the deputy head.
- The services and support of related administrative functions.
- Information on both departmental needs and security threats.
- Support in carrying out individual security responsibilities from all employees.

Within the security system there are policies, procedures and practices to support the co-ordination of physical security, personnel security and information technology security.

Outputs of the security system include:

- Application of safeguards to information and assets throughout their life cycle.
- Education of staff on their security responsibilities.
- Evaluation of the continued relevance of safeguards.

The systems concept of security offers flexibility within a standard approach. Threat and risk assessments should identify security factors unique to specific departments and locations. These factors should then be reflected in the specific safeguards chosen. For example, if required, an asset may receive more than the minimum protection for its classification level or designation.

Another feature of the systems concept is that, should any part of a system become inoperative or suspect, another part can be substituted, a temporary alternative installed, or another part of the system upgraded, to maintain integrity.

1.4 Guidance

For advice and assistance regarding this standard contact the organizations listed in Appendix A.

2. Organizing of security documentation

Government security documentation is organized in three tiers to provide increasingly detailed requirements and guidance. This structure can be viewed as a triangle, as in Chart 1, with the Security policy at the top, operational standards at the second level and technical documentation at the third, bottom level. The policy and operational standards are contained in the "Security" volume of the *Treasury Board Manual*. Technical (third-level) documentation is produced by the lead agencies responsible for the particular subject.

All security documentation evolves through a five-step process: needs identification and definition, response development, consultation and review, approval and promulgation. Responsibility for these steps is shown in Chart 2.

Chart 2: Security documentation - roles and responsibilities

Process	Security policy	Operational Standards	Technical Documentation
Needs identification	TBS	Lead agencies, coordinated by TBS	Lead agencies, coordinated by TBS
Response	TBS	Lead agencies,	Lead agencies,

Response	TBS	coordinated by TBS	coordinated by TBS
Review and consultation	Advisory committee	Advisory committee	Advisory committee
Approval	Treasury Board	Treasury Board or TBS	Lead agencies
Promulgation	TBS	TBS	Lead agencies

3. Organization of the security function

Each department is responsible for the organization and management of a security function that will allow the department to implement an effective security program and meet the requirements of the policy and its operational standards.

The effectiveness of the security function depends on the performance of each element, as described in the operational standards, and coordination between them. Departments should therefore organize the security function to provide for overall planning, budgeting, direction, co-ordination and evaluation. Decentralized organizations or branches with separate responsibilities, should use common procedures for such activities as classifying and designating information and assessing threats and risks.

Good general management provides the foundation for effective and efficient security. This is particularly true in the cases of screening and hiring personnel, planning accommodation and facility access control, and managing information technology systems and their security.

In some circumstances administrative practices alone may provide adequate protection for information and assets of lesser sensitivity. Where an assessment has shown the threat posed by deliberate efforts to obtain such information or assets is low, yet the threat posed by accident to be significant, special safeguards may not be required; care with administrative practices may be critical. For example, the minimum standard for the secure mailing of low-sensitive, designated information is to use a single envelope and first class mail, with the assumption that care will be taken to ensure use of a correct address. Similar examples exist in almost every aspect of administration.

Furthermore, administrative practices support and complement security safeguards, for whatever level of sensitivity. For example, the security of sensitive information on computers depends on good installation and operating practices as well as on safeguards.

It is therefore appropriate that the security function be positioned in the overall organization structure to facilitate coordination with and between program managers and those responsible for related administrative functions. Examples of related functions include managing information, information technology, contracts, property, materiel, finance, telecommunications, health and safety, fire protection, access to information and privacy, audit, and personnel.

For these reasons, the Security policy requires departments to appoint a departmental security officer (DSO) responsible for developing, implementing, maintaining, coordinating and monitoring a departmental security program consistent with the policy and its standards.

The DSO should have direct access to the deputy head to report probable security breaches or illegal acts, as warranted and in accordance with the DSO's Mandate.

To ensure effective communication between the different elements of security, functional relationships and reporting requirements should be set out in departmental policy.

Because of the important role played by the Minister's Office in the conduct of departmental business, the DSO should ensure an on-going working relationship with the officials responsible for the management of the Minister's Office. DSOs should also be familiar with the manual entitled Administrative Practices: Guidelines for Minister's Offices prepared by the Treasury Board Secretariat.

In summary, the organization of the security function should support the coordination of the elements of security, as well as coordination with related functions.

4. Information security

4.1 Reviewing information holdings

A thorough review of information holdings and assets, to identify material that requires either classification or designation, should precede the application of all security standards.

4.2 Information classification and designation guide

Departments must apply the information classification and designation system either by means of a corporate guide or by naming officials to do so or both.

This guide is the corporate policy about what information a department wishes its safeguards to cover. The guide shows:

- What types of information are considered sensitive.
- What types of information are not considered sensitive.
- How to mark information to show the minimum security standards to apply.

The guide should also identify officials to classify or designate information not governed by the guide. Departments should restrict the number of delegated authorities for this function and ensure that those exercising this authority have a demonstrable

and continuing need to exercise it.

Information that is publicly available is not to be classified or designated.

To develop a classification and designation guide, departments should follow the following process:

- Systematically review information holdings against the criteria set out in the guidelines in Appendix A to the Security policy.
- Assign the proper classification level to information sensitive in the national interest.
- Assign the proper designation level to information sensitive in other than the national interest.
- Whenever possible, determine the duration of classification or designation by showing the date or event that triggers declassification or downgrading.
- On a periodic basis, review with the departmental access to information and privacy coordinator decisions made to exempt information as a result of requests under the Access to Information Act and the Privacy Act. This is to ensure that departmental classification criteria remain relevant and effective.

4.3 Relationship to Access to Information and Privacy Acts

Most government information is adequately protected through good, basic information management and physical and materiel management procedures, without classification or designation. The Security policy requires departments to identify the relatively limited amount of government information that is sensitive and therefore merits additional protection. Identifying sensitive information relates directly to the exemption and exclusion criteria of the Access to Information Act and Privacy Act, which establish the legal authority for the information departments may refuse to the public.

Parliament has determined the information described in the exemption criteria to be important either to preserving the national interest or to protecting other interests for which the government assumes an obligation.

Cabinet confidences are excluded from the application of both Acts and qualify either for classification or designation.

In identifying information in need of additional safeguards, departments are not required to determine definitively whether specific items would actually be exempt under these Acts. A situation may change with circumstances and the passage of time. Rather, departments should be satisfied that various types of information could reasonably be expected to qualify for exemption. This judgment is to be based on a determination of potential injury and should be expressed in a departmental classification and designation guide.

The present security system is based on the notion that the government should not be using human and financial resources on additional safeguards for information unless it falls within the exemption or exclusion criteria of the Access to Information Act and the Privacy Act. The goal is to identify accurately the information the department has an obligation to protect, and then to determine the proper minimum safeguards.

Departments should examine carefully the guidelines in Appendix A to the Security policy, the specific provisions of the Access to Information Act and the Privacy Act, and the "Access to Information" and the "Privacy and Data Protection" volumes of the Treasury Board Manual to determine what information may qualify as classified or designated information and may therefore warrant safeguarding. Also, see Appendix C to this standard for additional guidance on classifying information affecting the national interest.

4.4 Types of designated information

Some special types of designated information are described below.

(a) Information received in confidence from other governments and organizations

This refers to unclassified information obtained in confidence from other governments or international organizations of states, as described in Section 13 of the *Access to Information Act* and Section 19 of the *Privacy Act*, and Chapter 2-8 of the "Access to Information" volume and Chapter 2-9 of the "Privacy and Data Protection" volume, *Treasury Board Manual*. This information may be marked "PROTECTED - other government." It is to be marked as received in confidence, with an indication of the source, before distribution to other departments. See articles 8.5 and 12.9 of this chapter for further information on this subject.

(b) Information obtained or prepared by a federal investigative body

This refers to law enforcement information obtained or prepared by specific investigative bodies named in the regulations pursuant to the *Access to Information Act* and the *Privacy Act*. (See para. 16(1)(a), ATIA, and para. 22(1)(a), *Privacy Act*). This information pertains to detection, prevention or suppression of crime or the enforcement of a law of Canada or a province. The specific federal investigative body involved will assign the level of protection. Departments receiving this information should give it equivalent protection, after consultation with the investigative body.

(c) Personal information

Personal information, as defined in Section 3 of the *Privacy Act*, qualifies for a mandatory exemption under the *Access to Information Act*. The *Privacy Act* refers only to personal information and imposes legal controls on its collection, use, retention, disclosure and disposal.

Personal information is found throughout the holdings of most departments. The formal reference for identifying personal information holdings is *Info Source*. This document responds to the requirement in the *Privacy Act* that makes each department responsible for listing each bank and class of personal information under its control.

Personal information includes information about public servants such as pay data, appraisals and medical information. Care should be taken not to confuse this type of sensitive information with information described in paragraph 3(j) of the *Privacy Act* (for example, classification level and salary range of public servants). This paragraph places certain limitations on the definition of personal information.

(d) Business information

Paragraphs 20(1)(a) and (b) of the *Access to Information Act* establish exemptions for the following types of information:

- Trade secrets of a third party.
- Financial, commercial, scientific or technical information that is confidential information supplied to a department by a third party and treated by it consistently as confidential.
- Information that could reasonably be expected to result in financial loss or gain to, or to prejudice the competitive position of a third party.
- Information the disclosure of which might reasonably be expected to interfere with contractual or other negotiations of a third party.
- Businesses or other organizations provide much of this information. There is an expectation on the part of the third party, and an obligation on the part of government departments, to protect this type of information adequately. It should therefore be designated as other sensitive information and marked PROTECTED.
- In some instances, third parties will mark such information confidential, confidential business information, or given in confidence. Departments should treat this information as if it bears the marking PROTECTED, regardless of the marking put on it by the third party.

(e) Advice

Section 21 of the *Access to Information Act* sets out exemptions for certain classes of information relating to the internal decision-making processes of government the disclosure of which would interfere with departmental operations.

Determination of injury or harm within the advice exemption should be judged on the basis of the impact disclosure will have on the department's and the government's ability to carry on similar internal decision-making processes, and to consult and deliberate in a confidential manner and to give candid advice.

The scope of information covered by this exemption is strictly limited. There is considerable difference between advice, recommendation, consultation or deliberation about a major government initiative and the purchase of office equipment. The best guide to exercising the discretion needed is common sense and good judgment.

It is also essential to bear in mind that, even though there is no exemption for advice in the *Privacy Act*, it is extremely important to protect advice given in deciding about individuals.

4.5 Gravity of injury

When information is classified in the national interest, a further judgment is needed to determine the classification level. The level depends on the gravity of the detrimental effects that might reasonably be expected to occur from compromise. The levels of classification are as follows:

- *Top secret:* applies to the very limited amount of information that, if compromised, could reasonably be expected to cause exceptionally grave injury to the national interest.
- *Secret:* applies to information that, if compromised, could reasonably be expected to cause serious injury to the national interest.
- *Confidential:* applies when compromise could reasonably be expected to cause injury to the national interest.

Most classified information will be at the confidential level.

In light of the broad concept of national interest and certain assumptions that can be made about generic threats, these classification levels call for the application of minimum standard safeguards, as well as additional safeguards based on departmental threat and risk assessments. Minimum standards are also required as a result of international agreements and arrangements concerning shared classified information.

There are three levels of designation:

- *Extremely sensitive*: applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the national interest, for example, loss of life.
- *Particularly sensitive*: applies to information that, if compromised, could reasonable be expected to cause serious injury outside the national interest, for example, loss of reputation or competitive advantage.
- *Low-sensitive*: applies to information that, if compromised, could reasonably be expected to cause injury outside the national interest, for example, disclosure of an exact salary figure.

Minimum standard safeguards also apply to the different levels of designated information. These safeguards differ from those that apply to classified information, based on differences in generic threat assessments. Also, owing to its unique nature in

each department, extremely sensitive, designated information warrants special safeguards based on case-by-case threat and risk assessment.

4.6 Particularly sensitive, personal information

A number of examples of personal information that may qualify as particularly sensitive are provided below. The listing should be treated as illustrative or supportive but not conclusive.

- Information containing medical, psychiatric or psychological descriptions.
- Information compiled and identifiable as part of an investigation into a possible violation of law.
- Information on the eligibility for social benefits or the determination of benefit levels (this would not include cheques or other such payment documents).
- Information on a completed income tax return.
- Information describing an individual's finances, that is, income, assets, liabilities, net worth, bank balances, financial history or activities, or creditworthiness.
- Information containing personal recommendations or evaluations, character references or personnel evaluations.
- Information concerning an individual's racial or ethnic origin or religious or political beliefs and associations or lifestyle.

Particularly sensitive, personal information exists in both large quantities throughout government and in large concentrations within certain departments. The high risk of theft or loss of this type of information means departments should take special care to properly identify it and to apply appropriate safeguards.

4.7 Invasion of privacy

For identifying particularly sensitive, personal information, the injury test is that the information's compromise could reasonably be presumed to cause an unwarranted invasion of privacy. Factors that should be taken into account in any invasion-of-privacy test include:

- Expectations of the individual.

Have certain conditions been placed on the collection of the personal information that would lead the individual to believe that special protective measures would be taken? Is the information of a nature such that the individual would expect the government to take very special protective measures without actually being informed that this would occur?

- Currency of the information.

Is the information very current and for that reason more sensitive, or has the passage of time possibly reduced that sensitivity so that disclosure under specific circumstances would lead to no measurable injury to the individual's privacy?

- Gravity of injury.

Can it be surmised that compromise of the information carries with it the chance of causing serious injury? Serious injury is to be interpreted as lasting harm or embarrassment that will have direct negative effects on an individual's career, reputation, financial position, safety, health or well-being.

There may be other factors unique to certain institutions that should be added to invasion-of-privacy considerations.

4.8 Collecting personal information

Personal information collected by departments requires protection throughout its life cycle. Examples of this type of information include interviews, reports, application forms, and questionnaires.

When a statistical study or survey involves processing personal information, the code that correlates data to an individual respondent must be destroyed as soon as possible, under a schedule approved by the National Archivist.

Contracts for the collection of personal information should include the following points:

- An undertaking to protect the information, to refrain from disclosure to any other person or organization and to use the information only for the purpose specified in the agreement.
- An undertaking to make the information available only to employees of the contractor who have undergone proper screening and have a need to know the information.
- That each employee to whom the information is made available shall sign a statement showing that he or she undertakes, as a condition of employment, to respect the sensitive nature of the information and to observe the requirements of the *Privacy Act* and any other conditions specified by the department governing the use of this information.
- That the department may terminate the contract if the contractor breaches confidentiality obligations.

See Chapter 2-5 for further information on contracting security.

5. Materiel asset security

According to the Security policy, materiel assets deemed to be sensitive in the national interest must be classified, while materiel assets with value or importance that warrants safeguarding must be designated. Examples of designated materiel assets include easily removed and sold articles, and equipment or building features that could attract vandalism. Both classified and designated materiel assets are referred to in this standard as "sensitive materiel assets."

Departmental policies should require the identification of sensitive materiel assets and their location, the type of safeguards that may apply and the name of their custodian. Custodians should be assigned responsibility areas for which they should report anything that they consider detrimental to the safekeeping of the asset. Users and custodians of sensitive materiel assets should be made responsible for safekeeping them during working hours and following procedures for safekeeping at all other times.

Procedures should require that all instances of damage to and confirmed loss of sensitive materiel assets are reported to the proper authority. Sensitive materiel assets should not be removed from government property nor from assigned custodial areas without proper authorization.

The Security Systems Branch of the RCMP will provide guidance on physical security for sensitive materiel assets, on request.

6. Information technology security

Information technology (IT) assets are a type of materiel asset; examples that may be designated as warranting safeguards include:

- IT information, software, hardware and facilities.
- IT services.
- Environmental support systems (for example, power and air conditioning).

Departmental security policies should require inventories of sensitive IT assets and assign accountability accordingly. Inventories should include an indication of the replacement and acquired value of IT assets, as this can serve as a useful criteria for the selection of safeguards. In addition, threat and risk assessments should include a statement of sensitivity to indicate confidentiality, integrity and availability attributes that warrant safeguarding.

See Chapter 2-3 for more information regarding information technology security.

7. Protecting personnel

The *Canada Labour Code* makes departments responsible for the safety and health of employees at work. (See Sections 124 and 125, Chapter L-2, *Canada Labour Code*, Part II.) Therefore, threat and risk assessments should include consideration of employees in roles where they may be subject to security threats. Examples of such roles include front-desk jobs where employees may encounter hostile or emotionally upset members of the public, and high-profile positions where employees may be threatened by severely disturbed persons or publicity seekers.

See Chapter 2-2 of this volume for references on protecting personnel.

8. Selecting safeguards

8.1 General

Departments must apply safeguards on the basis of threat and risk assessments, as well as security standards. This is to ensure consideration of the specific security problems in any given situation.

The risk management approach described below falls within the framework provided in the government Risk Management policy. For more information on this policy, see Part III of the "Materiel, Services and Risk Management" volume of the *Treasury Board Manual*.

8.2 Classified information and assets

The threat to classified information and assets may be greater in some situations or locations. Therefore, along with implementing minimum standards, steps must be taken to ensure adequate security. A threat and risk assessment is required to determine if and what additional safeguards are needed; these are to be implemented if it is cost-effective to do so.

Use of the markings "CONFIDENTIAL", "SECRET", and "TOP SECRET" signals the application of minimum standards.

In the absence of cost-effective safeguard options, the movement of sensitive information and assets to another, more secure site should be considered.

8.3 Designated information and assets

Minimum standard physical and information technology safeguards are used to protect information and assets that have been designated as being of low sensitivity or value. These safeguards protect against such threats as human error, inattention to proper procedures and mischief. An assessment is needed to be sure that the threat and risk are in fact minimal.

Use of the marking PROTECTED signals the application of minimum standards. Departments may use additional markings after PROTECTED to specify the requirement for minimum standards. Some departments add the letter A for this purpose.

To counter additional threats that may apply, more stringent safeguards are recommended for the protection of designated information that is particularly sensitive.

Departments have the option of adding the letter B to the marking PROTECTED to signal the need for additional safeguards. It cannot, however, be assumed from this mark that the application of safeguards will be identical from one department to another. The varying nature of particularly sensitive designated information and related threats will dictate safeguards appropriate to each situation.

Therefore, an assessment of security risks should be made when sharing particularly sensitive information on a regular basis. The department that collected or created the information is responsible for identifying the safeguards to be applied by the receiving department. If warranted, a written agreement should be developed with the DSO of the receiving department and should apply to third-party recipients of the information as well.

Furthermore, a very few departments hold designated information that if compromised may cause extremely serious injury such as loss of life or significant financial loss. Such information and assets could well be threatened by highly motivated and skilled individuals or organizations and, therefore, additional safeguards may be in order.

Departments have the option of adding the letter C to the marking PROTECTED to signal the need for special, stringent safeguards. Again, it cannot be assumed that the application of safeguards from one department to the next will be the same. The originating or collecting department should identify necessary safeguards and these should be agreed upon in writing. The written agreement should extend to third-party sharing of the information.

8.4 Limited examples of minimum safeguards

Limited examples of minimum safeguards for designated and classified information are provided in the following charts.

Chart 3: Limited examples of minimum safeguards for DESIGNATED INFORMATION

Activities	Low-sensitive	Particularly Sensitive	Extremely Sensitive
Personnel screening	Enhanced Reliability Check		
Paper handling and storage	Operations zone; container from *Securité Equipment Guide* or equivalent, based on TRA		
Mailing in Canada	Single envelope; lst class mail		With conditions attached: mail, messenger, courier or authorized person
Paper destruction	Hand shred	Shredder, as listed in *Security Equipment Guide*	
Facsimile transmission	Ensure receiving fax machine in Operations Zone		Ensure receiving secure fax machine in Security Zone, with confirmed recipient present
Telephone conversations	Threat and risk assessment by user		Use secure phone (Type I or II STU III) in appropriate location
Personal computer use on networks	Threat and risk assessment by manger and user	Discretionary or mandatory physical and IT access controls, based on TRA	Mandatory physical and IT access controls, approved cryptography

More comprehensive guidance is available in operational and technical standards. Threat and risk assessments should be used to determine the need for more stringent safeguards.

Chart 4: Limited examples of minimum safeguards for CLASSIFIED information

	Confidential	Secret	Top Secret
Personnel screening	Level 1 security clearances	Level II security clearance	Level III security clearance
Paper handling and storage	Operations zone, container from *Security Equipment Guide,* based on TRA		Security zone; container from *Security Equipment Guide,* based on TRA
Mailing in Canada	Single envelope; lst class mail		With conditions attached: mail messenger, courier or authorized person
Paper destruction	Shredder, as listed in *Security Equipment Guide*		
Facsimile transmission	Ensure receiving secure fax machine in Operations Zone with confirmed recipient present.		Ensure receiving secure fax machine in Security Zone, with confirmed recipient present.
Telephone conversations	Secure phone (Type I STU III) in appropriate location		
Personal computer use on networks	Mandatory physical and IT access controls; approved cryptography		

More comprehensive guidance is available in operational and technical standards.
Threat and risk assessments should be used to determine the need for more stringent safeguards.

8.5 Information from other governments

Departments must treat sensitive information received from other governments or from international organizations in accordance with the security markings on it or with agreements or understandings between the parties concerned.

"Other governments" include provincial, municipal or regional governments and those of other nations.

9. Managing security risks

9.1 General

Risk management is a logical, analytical process to protect, and consequently minimize risks to, the government's property, interests and employees. The Risk Management policy requires departments to identify, analyze and assess risks, select risk-avoidance options, and design and implement cost-effective prevention and control measures. Departments are also required to design and implement contingency plans, as appropriate. For further information on this policy, see the "Materiel, Services and Risk Management" volume of the *Treasury Board Manual*.

In the security context, the risk management process offers the following options:

- Reduce risk, for example by improving security.
- Avoid risk, for example by changing operations.
- Remove or reduce safeguards that are not required.
- Contain risk by preparing business resumption plans.
- Accept risk on an informed basis, as appropriate.

The Security policy requires departments to complete threat and risk assessments (TRA) for sensitive information and assets as part of the risk management approach to security. The threat and risk assessment process is a part of risk management concerned with defining what requires protection, analyzing and assessing threats, analyzing and assessing risks, and making recommendations for the management of risk. Other aspects of risk management are management decision, implementation and effectiveness review.

The system to manage a security risk should be compatible with those for managing other risk in the same area, for example, fire.

9.2 Assessing threats and risks

It is the nature of threats that provides the main design criteria for security systems and equipment. Furthermore, security systems and equipment have useful life spans often dictated by the technological advances available to the potential adversary. A complete and current assessment of the threat to information and assets is therefore needed to determine the adequacy of existing or proposed safeguards.

Inappropriate safeguards may leave the information or asset to be protected vulnerable to identified threats or, conversely, it may be overprotected. It is the role of security officials to assess the chance of vulnerabilities being exploited by a threat (that is, the risk). They should then recommend ways of managing risks by means such as risk acceptance, moving the information or asset, eliminating the threat, increasing protection, upgrading detection and response mechanisms, and preparing contingency plans.

A threat and risk assessment should be completed for the entire department, as well as for specific facilities, areas, systems or functions. Depending on the structure of the department, the general departmental assessment should combine and analyze specific assessments. Additionally, the general assessment should address those threats that may affect the department as a whole, or pose a threat to its facilities, areas, systems or functions. This process will result in a comprehensive and complete assessment suitable for briefing the deputy head, as required.

Information on a general threat should be made available in a timely fashion to those responsible for specific assessments. An example of such a general threat is events that might occur as the result of planned changes in the legislation affecting the department's programs.

Specific assessments should be detailed enough to serve as the basis for recommendations to the responsible manager. Safety and emergency considerations must be taken into account in such assessments.

Threat and risk assessments should be reviewed on a regular basis and revised when there are circumstances that could result in a changed threat. Examples of changes in circumstance include the introduction of new policies or new technology, relocation, or reorganization.

The process that follows is not intended to limit a department's own security operation nor to restrict its access to sources of threat and risk information.

See article 2.3 of Chapter 2-3 for information on the threat and risk assessment process for information technology.

9.3 Process

The development of a threat and risk assessment includes four broad steps:

- Preparation: determining what to protect and defining the scope of the assessment.

- Threat assessment: determining what to protect against.
- Risk assessment: determining if existing or proposed safeguards are appropriate.
- Recommendations: identifying what should be done to provide appropriate protection.

An outline of each of these steps is provided below.

Preparation

The first step is to identify the types of information and assets that may require safeguarding and the scope of the assessment.

A statement of the nature of the business carried out by the organization will assist in the identification of information or asset sensitivity, importance and value.

Threat assessment

Threats specific to classified information and assets should be examined to verify if conditions of minimum threat apply. Where minimum threat conditions apply, the next step is to assess the implementation of the minimum safeguards prescribed in the standards. Special conditions that could warrant additional or different safeguards apply where, for example, classified information and assets are targeted or located in a hostile environment.

Threats specific to designated information and assets, personnel, information systems or services should be described in detail. Use of the standard investigative questions who, what, when, where, why, and how is recommended. Departmental security records should be consulted for information on security infractions and violations. Also information regarding the experience at similar or neighbouring facilities or systems should be obtained.

Close attention should be paid to times or handling processes during which the information or asset is most vulnerable (for example, during periods between public access and restricted access hours or while in transit).

If possible, the specific threat assessment should include any threat information that pertains to the department as a whole and should be reviewed by a regional or departmental security official.

Advice on threats is available from several sources, including the following:

- CSIS, for assessments of espionage, sabotage or terrorism threats, as specified in Section 2 of the *CSIS Act*, to departmental information and assets.
- The RCMP, for threat information and advice on threat and risk assessments related to criminal matters, physical security, computer security and other relevant aspects of information technology security.
- CSE, for technical threat information relating to COMSEC and other relevant aspects of information technology security.

See Appendix A for the addresses of these organizations.

Departments with facilities abroad containing sensitive information and assets should maintain liaison with the Department of Foreign Affairs and International Trade through their security office. The managers responsible for health, safety and emergency preparedness should be consulted regarding threats that are also a security concern, such as fire.

Next, the likelihood and consequences of a threat occurring should be assessed.

Likelihood

The likelihood of the threat occurring should be evaluated in terms of "low", "medium" or "high." Low means there is no history and the threat is considered unlikely to occur. Medium means there is some history and an assessment that the threat may occur. High means there is a significant history and an assessment that the threat is quite likely to occur. The term "not applicable" may be used to indicate that a threat is considered not to be relevant to the situation under review.

There are various methods for assigning numerical values for estimated levels of threat. Often, however, these methods can easily become complicated and they may require interpretation to become meaningful. Therefore, the use of descriptive terms is recommended.

Consequences

Having considered the likelihood of a threat occurring, it can then be useful to state what consequences would result. This is a restatement of the assessment made when classifying and designating information and assets regarding the potential injury compromise might cause.

In the case of classified information and assets, the consequences of compromise are expressed in terms that relate to the classification level: serious injury, very serious injury or exceptionally grave injury.

For designated information and assets, personnel and services, consequences should be expressed in terms such as "loss of trust", "loss of privacy", "loss of asset", or "loss of service."

Risk assessment

The next step is to evaluate vulnerabilities that may permit a threat to cause harm. Assess existing and proposed safeguards as completely satisfactory; satisfactory in most aspects; or unsatisfactory.

Use of a departmental checklist of standard safeguards is recommended. If some aspects of the security system remain unassessed, this should be recorded.

Help in assessing safeguards may be obtained from the lead agencies. Ideally, before requesting help with this step, the threat assessment will have been completed. Where this has not been possible, assistance with the entire process should be requested.

Recommendations

The threat and risk assessment should result in a report to management. The report should provide recommendations in order of priority to reduce or eliminate security risks. It should also indicate resource implications, including finances, personnel, equipment and time.

A useful threat and risk assessment is one that provides the manager with an appreciation of the security status of the area or system concerned. The TRA should enable the manager to make an informed decision on safeguards to be applied or removed.

To illustrate the use of the threat and risk assessment terminology, an example of an outline is provided on the following page.

Sample Threat and Risk Assessment Summary

Facility: District Office. **Business**: Administration of benefit program. Clients are interviewed in an operations zone.

Information/Assets: Particularly sensitive, personal information on both paper and electronic files.

Location of Assets: Approved containers within a security zone. Office is in downtown area; a move is planned.**Threats**:

Sample Threat and Risk Assessment

Vandalism:	• Low - Minor delay in service.
Theft:	• Low - Loss of service, confidentiality, trust.
Computer failure:	• Medium - Loss of service and trust. • Loss during planned move; • Medium -Loss of service and trust.

RISK: Generally low risk since existing security measures are satisfactory. Exceptions:

- Medium risk of loss due to computer failure in view of unsatisfactory computer backup procedures.
- Medium risk of loss during planned move due to lack of procedures for secure transfer of files to new location.

Recommendations:

- Develop and implement computer backup procedures.
- Develop and implement procedures for security of paper files during the planned move.

Note: Greater detail on the nature of threats and on security measures should be available in supporting documentation

10. Need to know

A fundamental requirement of the Security policy is to limit access to sensitive information to those whose duties require such access; that is, to those who need to know the information. While personnel screening levels potentially provide access to levels of sensitive information, application of the need-to-know principle restricts access within those levels to specific items, topics or types of sensitive information. Personnel are not entitled to access merely because it would be convenient for them to know or because of status, rank, office or level of clearance.

The need-to-know principle may be implemented in various ways. These include physically segregating and controlling access to the information, producing lists of those who may access certain types of information, marking information to specify who may or may not access it and installing mandatory or discretionary access controls on information technology systems.

Other means to control access distribution include compartmentalization of sensitive information combined with detailed security briefings, known as indoctrination, debriefings, and the written undertaking of related security responsibilities.

The department originating or acquiring sensitive information and assets is responsible for the application of the need-to-know principle.

11. Marking information

Classified information must be marked or otherwise identified at the time it is created or collected, to alert those who use it that it requires protection at the applicable level.

Designated information should be marked at the time it is created or collected.

Further, *designated information must be marked if it is to be disclosed beyond the organizational unit that created or collected it.* The only exception is routine information exchanged with the individual or organization that is the subject of the information. For instance, there is no need to mark a cheque sent to an individual or his or her official representative.

See Appendix D for additional information on the security marking of sensitive information.

12. Declassifying and downgrading

12.1 General

Information must be classified or designated only for the time it requires protection, after which it is to be declassified or downgraded.

This requirement recognizes that classified or designated information will lose its sensitivity with the passage of time or the occurrence of specific events. When releasing such information is unlikely to pose injury to the particular interest involved, as described in the appropriate provisions of the *Access to Information Act* and the *Privacy Act*, it must be declassified. This process contributes to the overall integrity of the security system, and ensures that information is made available quickly and informally to interested members of the public.

The departmental classification and designation guide should confer authority to declassify or downgrade information.

12.2 Automatic declassification and downgrading

Departments should provide, whenever possible, for automatic declassification or downgrading of information by selecting a specific date or event for its declassification or downgrading at the time the information is created or collected.

Along with date or event-specific triggers for declassification, an automatic expiry date of 10 years should apply to secret, confidential and low-sensitive designated information. However, an automatic expiry date would not apply to information classified as top secret nor to information designated as particularly sensitive (e.g., medical records) or extremely sensitive (e.g., witness protection information).

The risks associated with the use of an automatic expiry date are acceptable because removing material from the classification scheme is not synonymous with making it publicly available. The normal access application review process would still apply.

12.3 Shared information

The requirement to declassify or downgrade sensitive information applies also to that provided from one department to another. Where possible, *before declassifying or downgrading any information orginating from another department, the originator must be consulted*. The originator can be represented by the office of origin.

Information may be transferred to the department or government that originated it for declassification or downgrading. In most circumstances, however, it will be more practical, especially with a large volume of information simply to consult the other department or government about whether it is appropriate to declassify or downgrade the information.

When it is not possible to consult with the originator, departments should develop alternative procedures and include these in their classification and designation guides. This will be necessary, for example, when the originating department has been disbanded or reorganized in such a way as to make it impossible to consult effectively or efficiently with the originator.

A decision to declassify a document from another department should not be taken lightly. Where consultation with the originator is impractical or not possible, and there is doubt regarding the continued need for protection, procedures should require consultation with the appropriate officials. For example, the Access to Information Co-ordinator will be able to advise on whether exemptions or exclusions may still apply.

12.4 Access requests

Requests under the Acts for records that have been classified or designated should involve careful review of the information by the departmental access and privacy coordinator in conjunction with the appropriate areas. The review should determine whether any exemptions should be invoked and whether there is a need for interdepartmental consultation.

A decision to deny access to a record, or any part of it, must be based solely on the exemption provisions of the Acts as they apply at the time of the request. A decision to deny access must not be based on security classification or designation, however recently it may have been assigned.

The principle of severability applies to information requested under both Acts. It may happen that classified or designated information is severed from a document as a result of review when responding to an access request. The original document, of which a severed copy has been released, remains classified or designated. *When no severance occurs and a whole document is released, it must be declassified before its release and marked accordingly.*

Personal information disclosed under the *Privacy Act* is to be reviewedCsuch information may keep its designation as sensitive information within the information holdings of the department.

In light of decisions made as a result of requests made under the Acts, a periodic review should be made of the departmental information classification guide.

12.5 Transfer of functions

Where sensitive information moves with a transfer of functions, the receiving department is deemed to be the originating department.

12.6 Information transferred to the National Archives of Canada

Departments are expected to transfer to the control of National Archives of Canada sensitive information for which the retention period has expired and which the National Archivist has identified as having enduring historical or archival value.

Departments must develop with the National Archives of Canada agreements to declassify or downgrade sensitive information transferred to the control of the Archives. These agreements are to take into account guidance provided by the originating departments, that will indicate where consultation between the Archives and the department is necessary.

The above does not apply to dormant records stored in the records centres of the National Archives. Control of such records remains with the department storing the information.

12.7 Defunct departments

In situations where a department ceases to exist and its functions are not transferred to a successor department, records of the defunct organization must be transferred to the National Archives of Canada for eventual declassification or downgrading.

For information that originated with a defunct department, each department in control of copies of such information is deemed to be the originating department. Such information may be declassified or downgraded by the department that controls it, after consultation with any other department that has an interest in the information.

12.8 Review

Departments should encourage users or originators of sensitive information to review its sensitivity on a continuing basis. *Where appropriate, the information is to be declassified or downgraded and marked accordingly.*

12.9 Information from other governments

Classified information received from provincial, municipal or regional governments, from governments of other nations, or from international organizations must be declassified or downgraded under agreements or understandings with such governments or organizations. For example, the convention governing classified information of the British government received by the Government of Canada is that such information is not considered for declassification until 30 years after its creation.

When consulting on declassification or downgrading with a foreign government or international organization, government departments should normally coordinate such consultations through the Security Services Division, Department of Foreign Affairs and International Trade. Direct consultation should take place only when an established and acceptable system of liaison and consultation exists. The Department of Foreign Affairs and International Trade should be kept informed of these consultations.

12.10 Classified cryptographic information

The Communications Security Establishment is responsible for establishing, in consultation with affected departments, procedures for systematically reviewing classified cryptographic information for declassification or downgrading. *Departments must consult CSE before downgrading or releasing to the public COMSEC information or materiel that CSE has produced, issued or released.* This includes information or materiel from before 1975 when CSE was the Communications Branch of the National Research Council (CBNRC).

12.11 Classified security intelligence information

The Canadian Security Intelligence Service is responsible for establishing, in consultation with affected departments, special guidelines, procedures and practices for systematically reviewing for declassification or downgrading classified information about intelligence activities, as defined in the *Canadian Security Intelligence Service Act*, as well as information about

intelligence sources or methods. Where appropriate, the Communications Security Establishment, the Department of National Defence, Privy Council Office and the Department of Foreign Affairs and International Trade are responsible for establishing such guidelines, procedures and practices for classified information that they have originated or have under their control.

12.12 Confidences of the Queen's Privy Council

Confidences of the Queen's Privy Council for Canada that are classified and records that are administered under the Cabinet Papers System remain classified if they have been in existence for less than 20 years. Only in very rare instances will such records be declassified or downgraded before they have been in existence for 20 years. After 20 years, these records can be declassified or downgraded pursuant to this section of the security standards.

12.13 Revision of marking

Changes to a security marking should be made in ink, dated and initialed by the authority responsible for the change. Where there is documented authority for a change in security marking, this should be noted on the record. This applies particularly to records originating with other governments, other departments or international organizations.

For information stored in non-textual forms (such as computer data), revisions to security markings should be adapted to the particular application. Usually this will involve marking the container holding the information. Wherever technically possible, however, departments should mark the information itself in a non-erasable format.

13. Sharing sensitive information with other governments and organizations

Departments must ensure, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations. ("Other governments and organizations" refers to those not subject to the Security policy but with whom sensitive information is shared).

In most cases, it is expected there will be in place a general agreement between the federal government and the other government or organizations involved. The agreement should represent an undertaking to safeguard information appropriately, to limit use, to control release to third parties and to inform authorized users of their responsibilities under the agreement.

Without such a general agreement, arrangements for sharing information should be stipulated in an agreement between the originating federal department and the provincial government or department concerned.

Such agreements for sharing information should include the following elements:

- A description of the types of information to be shared.
- The purposes for which the information is being shared.
- A stipulation that the information is to be distributed only on a need-to-know basis within a recipient department.
- A description of all the administrative, technical and physical safeguards required to protect the information involved.
- A requirement that the recipient maintain a list of all officials, by position, who have access to the information.
- The conditions for disclosing information to third parties.
- The name, title and signature of the appropriate officials in both the originating department and the receiving province and the period covered by the agreement.

These elements should be considered for agreements according to the degree of injury that could result if the information were compromised.

Conditions for disclosure to third parties referred to above include obtaining the authority of the originating federal department in all cases before disclosing the information to third parties. Another condition is that such disclosure must be made under the terms and conditions specified by the originating department. Further, the agreement should warn that failure to abide by this provision will lead to an end of the sharing of such information.

Limited circumstances exist where confidential or secret information may be provided to outside organizations without the requirement for a security clearance. Examples include programs approved by the deputy head for the sharing of classified information with provincial governments. Under no circumstances is top secret information to be provided without the recipient being security cleared at Level III.

Note that Chapter 3-5 of the "Privacy and Data Protection" volume of the *Treasury Board Manual* sets out the components for agreements when sharing personal information with foreign governments, international and provincial organizations. Subsection 8(2) of the *Privacy Act* imposes special conditions on the sharing of personal information. These conditions are discussed in Section 6 of the "Privacy and Data Protection" volume. The components for these agreements can, however, be adjusted appropriately to consider third party business information, law enforcement information, and the like, to deal with situations outside the *Privacy Act*.

14. Telework security

The government Telework policy enables employees, with the agreement of their manager, to work at locations other than their official workplace. For further information on telework, see the Telework policy, Chapter 2-4 in the "Human Resources" volume of the *Treasury Board Manual*.

The Telework policy does not diminish responsibilities for the security of sensitive information and assets. Accordingly, departments

should arrange to advise and assist managers and employees in minimizing the risks inherent in working with sensitive information away from the official workplace.

Given the high risks involved, telework should not involve access to information that is designated as extremely sensitive or classified as top secret. Departmental policies should provide guidance on employees' access to other sensitive information that they require when they are teleworking.

Assistance to employees should involve briefing them on aspects of the safe custody and control of sensitive information and making the necessary arrangements for them to be able to meet their obligations.

15. Security awareness training

Security awareness training is an essential component of a comprehensive and effective security program.

Such training is a continuing series of activities, with two overall objectives:

- Keeping staff aware of their responsibilities and the part they must play in implementing and maintaining security within the department.
- Gaining and maintaining the commitment of staff to, and acceptance of, those responsibilities and actions.

Awareness training creates a sensitivity to threats and provides details on departmental policy and procedures for protecting departmental information and assets. It should be impressed upon staff at all levels that security is part of their everyday duties, rather than an optional extra or someone else's job.

To be effective, awareness training must be continually reinforced. Security officers may find it a useful practice to circulate departmental regulations periodically through newsletters or bulletins to all personnel and to conduct lectures from time to time on various security subjects.

16. Inspections and investigations

16.1 General

Ensuring compliance with safeguards should be part of normal administrative and supervisory duties, complemented by periodic or regular inspections of sites or systems where sensitive information and assets are processed or stored. Inspections might also be carried out as part of controlling access at transition points. Characteristically, security inspections are routine and random in nature; they are not directed at specific employees, on the other hand, security investigations are related to specific events and therefore may focus on certain employees. Examples of inspection activities include checking office areas during limited-access hours, keystroke monitoring of information systems, auditing of user access to systems and the use of closed-circuit television. Security breaches and violations should be investigated as a basis for remedial action and for reporting to the appropriate authorities, as required.

Inspections should be conducted by personnel or security guards (where employed) at the end of normal working hours and by persons assigned to the organizational unit workplaces at the beginning and end of work periods.

Suspected violations or breaches of security should be reported without delay and remedial action should be taken to avoid having a continuation of the problem.

16.2 Personal privacy

The *Canadian Charter of Rights and Freedoms* guarantees that government employees have a right to a reasonable expectation of personal privacy; and this right extends to the workplace. They also have protection under the *Privacy Act.* A security inspection or investigation in the workplace , including any search or seizure, must respect this right and be balanced with the department's need for supervision, control and efficient operation of the workplace. If a proper balance is not struck, and a search or seizure is found to be unreasonable, any evidence obtained may not be admissible in court. Moreover, the department may be liable for any damages, civil or criminal, that result.

What is "reasonable" will depend on the circumstances in each case, and may vary from department to department, depending *inter alia* on specific responsibilities and activities, the nature of the work site and the purpose of the inspection or investigation. If challenged, the onus will be on the department to show that a particular search or seizure was reasonable. A departmental security policy that clearly sets out the conditions under which searches or seizures will be carried out, would be important evidence in such a case.

16.3 Policies and procedures

Departments conducting security inspections and investigations must have policies that establish the conditions under which these will be carried out. Security inspection policies and procedures must be clear, unequivocal and comprehensive; reasonable in the circumstances; and brought to the attention of employees before being implemented. They must also conform with the collective bargaining regime or any collective agreement in force.

Informing employees of inspection and investigation policies and procedures before they are implemented means giving reasonable notice to existing employees and advice on application or commencement for new employees. Where appropriate,

the consent of the affected individuals should be obtained.

There is a need for prudence where inspections begin to merge with criminal investigations. That is, inspections are to be confined to the conditions set out in departmental policies; they are not to be deliberately used to by-pass the procedural requirements of the criminal law. In particular, inspections should not be used as a pretext for carrying out a search for or to gather evidence of criminal wrong-doing without reasonable grounds.

Policies should require that security breaches and violations be reported promptly and procedures should explain how and to whom such reports should be made.

Employees should also be informed of the reasons for inspection and investigation policies and procedures and their cooperation in implementing them should be encouraged.

Departmental inspection and investigation policies should be reviewed by departmental legal services before implementation.

16.4 Breaches of security

Departments must establish policies and procedures for dealing with breaches of security. These policies and procedures should cover the following points:

- The immediate reporting to the deputy head of possible breaches of security.
- The immediate reporting to CSIS of probable breaches of security involving classified information or assets.
- Reporting to the appropriate law enforcement authority breaches suspected of constituting criminal offences.
- Where applicable, informing the department that originated the information or other assets involved that a breach of security has occurred.
- Informing other departments that have information or assets involved in a breach of security of the circumstances and findings that affect them.
- Assessing injury as soon as possible whenever it is probable that a breach of security has occurred and reporting this to the deputy head.

Clearly minor incidents need not be reported to CSIS; the potential injury to the national interest should be taken into account in such cases. Reports should be made through the DSO. To report probable breaches to CSIS, use the address and telephone number listed in Appendix A.

16.5 Criminal offences

Suspected cases of theft, fraud, defalcation or any other offence or illegal act that involves employees and that do not require an immediate response by a police agency may be referred to departmental legal services for an opinion on the seriousness of the incident before taking further action. Otherwise, government policy requires that all losses of money and suspected cases of fraud, defalcation or any other offence or illegal act against the Crown must be reported to law-enforcement authorities. For further information, see Chapter 8 of the "Financial Management" volume of the *Treasury Board Manual*.

16.6 Searches in criminal investigations

All search requirements connected with an investigation into a suspected or potential criminal offence must be reviewed by a departmental security officer in consultation with departmental legal services and local police. A warrant is to be obtained where and when legally required.

16.7 Disclosing sensitive information

Occasionally, circumstances surrounding a search might expose sensitive information to investigators and other persons who are not authorized to have access to sensitive information. In these cases, the departmental security officer, in consultation with the manager, should review the sensitivity of the information and take action consistent with the requirements of the investigation and the intent of the Security policy.

The above circumstances involve difficulties that might require special screening status, legal consultation and executive authority to resolve.

16.8 Evidence

In all instances where sensitive information might fall under public scrutiny as a result of judicial action, the departmental security officer must consult with departmental legal services.

Departmental personnel who might be required to testify or give evidence in a legal proceeding connected with a criminal offence should document such matters to support any testimony required from them.

16.9 Investigative cooperation

It is often necessary for departments, police and other agencies to cooperate to achieve a thorough inquiry. Where appropriate, protocols should be established to regulate these cooperative requirements and departments should incorporate them into their policies and procedures. However, such protocols, policies and procedures are not to be used as substitutes for or means of bypassing warrant or other constitutional requirements.

16.10 Testing security systems

Periodic tests of security procedures, plans and equipment should be undertaken, but only with due regard to the possible negative consequences of inappropriate responses. Such tests might include entering an alarmed controlled area or security zone to test an electronic detection device.

Supervisory personnel should be advised of planned tests and evaluations that will affect security measures.

Developmental exercises designed and employed to assess security capabilities and the levels of knowledge and awareness of employees should be considered when incidents suggest that weaknesses exist, or to strengthen the effectiveness of the security program.

17. Managing security guards

Departments are responsible for determining the requirement for and the funding of security guards for the safeguarding of information and assets.

Custodian departments are responsible, on a site-specific basis and with reference to a threat and risk assessment, for providing and funding guards to protect facilities.

Every effort should be made to reduce guard costs through the effective design of new buildings and floor layouts and the use of other protective methods.

Further to the requirements of the Security policy, guards must be appropriately security screened, depending on their possible access to sensitive information and assets. This does not refer to access resulting only from the discovery of a security breach.

Public Works and Government Services Canada is responsible for providing advice and guidance on the contracting and screening of guards.

See Appendix B for a list of reference documents.

Appendix A - Guidance

General

Enquiries about this standard should be directed to the responsible officers in departmental headquarters, who, in turn, may seek interpretation from the Security and Identity Management Division.

Sources of threat assessment information

For assessments of espionage, sabotage or terrorism threats, as specified in Section 2 of the CSIS Act, to departmental information and assets, contact:

Assistant Director
Requirements and Analysis
Canadian Security Intelligence Service
P.O. Box 9732
Station T
Ottawa, Ontario
K1G 4G4

Telephone: 613-782-0243
(24-hour service)

For threat information and advice on threat and risk assessments related to criminal matters, physical security, and general aspects of information technology security contact:

Officer in Charge
Security Systems
RCMP
1200 Vanier Parkway
Ottawa, Ontario
K1A 0R2
Telephone: 613-993-7977
Facsimile: 613-952-5512

For technical threat information relating to COMSEC and other relevant aspects of information technology security, contact:

Head

TRANSEC and Operation Support
Communications Security Establishment
P.O. Box 9703
Ottawa Postal Terminal
Ottawa, Ontario
K1G 3Z4
Telephone: 613-991-7482

Appendix B - References

- "Access to Information" volume, *Treasury Board Manual*
- *Administrative Practices: Guidelines for Ministers' Offices*, Treasury Board Secretariat
- *Guide to Managing Guard Services* (SSB/SG-29), Royal Canadian Mounted Police, 1993
- "Information Management" volume, *Treasury Board Manual*
- "Materiel, Services and Risk Management" volume, *Treasury Board Manual*
- "Privacy and Data Protection" volume, *Treasury Board Manual*
- *Security Guards, Uniformed* (CAN/CGSB133.1-87), Canadian General Standards Board
- *Security Guards, Supervisors* (CAN/CGSB133.2-92), Canadian General Standards Board
- Telework policy, Chapter 2-4, "Human Resources" volume, *Treasury Board Manual*
- Security Services - Commissionaires and other Guards, Chapter 370, *Customer Manual* (Materiel Management), Government Services Canada

Appendix C - Classifying Information Affecting the National Interest

Administrative security within the government of Canada has traditionally been based on classification system for sensitive information and assets. This system has been misused to classify other than information related to the national interest, impairing the effectiveness of safeguards to protect sensitive government information and leading to unwarranted safeguards including the screening of individuals. In classifying information, departments should take care to balance the risk of injury to the national interest against the cost of safeguarding information at high levels of classification.

There is a very limited amount of information held by departments that warrants classification in the national interest. The threshold at which injury to the national interest would be occasioned must be closely monitored and circumscribed to avoid any dilution that could lead to an undermining of the credibility of the overall classification system. What counts is the content of the record, the substance of the information. The following guidance provides a basis for determining when information would fall within the national interest category.

Federal-provincial affairs (s. 14, ATIA)

Information where compromise could reasonably be expected to be injurious to the conduct by the Government of Canada of federal-provincial affairs. The exemption aims at preserving the federal government's role only, not the whole spectrum of federal-provincial relations. This will normally relate to federal-provincial consultations and deliberations and to strategy and tactics adopted for the conduct of federal-provincial affairs for the government as a whole where divisions of powers and the forms of government are under consideration (e.g., the constitutional negotiations).

This category does not cover the myriad of federal-provincial activities carried on by the majority of departments. These may well qualify for exemption from access under the Access to Information Act. Adequate protection can be provided under the designated category.

International affairs and defence (s. 15, ATIA)

Information where the compromise could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities. This category encompasses the traditional national security concern where the disclosure of information would be detrimental to the safety and security of the nation. Examples of documentation falling into this category:

- Diplomatic plans and negotiations whose essential purpose is the maintenance of the safety and security of the nation.
- Aspects of negotiating processes (e.g., strategy, tactics, and positions) which would give another nation unfair advantage.
- Analyses of, or commentaries on, the domestic affairs of another nation, the disclosure of which would not be in Canada's interest.
- Diplomatic correspondence exchanged with foreign states or international organizations of states or official correspondence exchanged with Canadian diplomatic missions or consular posts abroad. Quite likely much official correspondence would not be classified such as correspondence on the internal administration of missions and cultural and public information programs.
- Tactical and strategic defence plans, operations or exercises, including the characteristics of equipment and military techniques and the scale, movement and placement of forces.
- Information obtained or prepared for the purpose of intelligence relating to defence or the detection, prevention or suppression of subversive or hostile activities. This encompasses both raw data (information obtained) as well as the refined product or analysis (information prepared).
- Methods of, and scientific or technical equipment for, collecting, assessing or handling information relating to international relations, defence and security and intelligence.
- Communications or cryptographic systems of Canada or foreign states used in the conduct of international affairs, the defence

of Canada or states allied or associated with Canada, or in relation to the detection, prevention or suppression of subversive or hostile activities.
- Lawful investigations into activities suspected of being threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act* and investigative techniques and plans for such investigations.

Given the nature of the information involved, it would normally be found in the Privy Council Office, the Department of Foreign Affairs and International Trade, the Department of National Defence and the national security and intelligence agencies.

Investigations pertaining to the security of Canada (paragraphs 16(1)(a)(iii), 16(1)(b) and 16(1)(c) ATIA)

Information qualifying for classification under this category is very restrictive in that the information must relate to threats to the security of Canada described in Section 2 of the *Canadian Security Intelligence Service Act*. Only a limited number of departments hold such information, most notably the CSIS and the RCMP.

To qualify for classification the information must meet the following criteria:

- The information was obtained or prepared by those limited number of investigative bodies, listed in regulations made pursuant to the access or privacy legislation.
- The information was obtained or prepared during a lawful investigation.
- The information pertains to activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*.

Information relating to investigative techniques or plans for specific lawful investigations in relation to the above would also qualify for classification in the national interest.

Economic Interests of Canada (paragraphs 18(a) and (d), ATIA)

This section has two parts. The first relates to trade secrets or financial, commercial, scientific or technical information that belongs to the Government of Canada or a government institution and has or is likely to have substantial value. There exists information and technology relating to nuclear, biological or chemical weaponry that deserves classified protection. As well, there is specialized government scientific and high technology research in areas that may need to be safeguarded in the national interest. Examples include advanced communications, electronics, chemical technology and biotechnology, including military applications.

It should be noted, however, that this is a small part of overall government scientific and technical research, which is generally aimed at promoting national industrial development and economic competitiveness. Often research and development are carried on in partnership with the private sector and the information itself is relatively public in nature. Except for that small portion of such information that may require classification, the remainder, which is sensitive, is adequately safeguarded as designated material.

The second part relates to information where disclosure could reasonably be expected to be materially injurious to the financial interests of the Government of Canada and its ability to manage the economy. Examples are information relating to the following subjects:

- The currency, coinage or legal tender of Canada.
- Contemplated changes in tariff rates, taxes, duties or any other revenue source.
- Contemplated changes in the conditions of operation of financial institutions.
- Contemplated sale or purchase of securities or of foreign or Canadian currency.

This category is intended to cover management of the national economy. Such information would normally be found in the Department of Finance, the Bank of Canada, and Revenue Canada.

Appendix D - Marking Sensitive Information

Suggested procedures for marking and controlling sensitive information are as follows:

Top secret information

Mark TOP SECRET in the upper right corner of each page and show the total number of pages on all pages. Assign a unique whole number to each copy, mark the copy number on each page and maintain a distribution list. Further copies of top secret information should be made only if the recipient of an original assigns a unique identifier to each subsequent copy and maintains a distribution list.

Secret information

Mark SECRET in the upper right corner of each page. Number each copy, show the copy number on the face of each copy and maintain a distribution list.

Confidential information

Mark CONFIDENTIAL in the upper right corner of the face of the document. Control copies of confidential documents in the same way as secret documents, when warranted by a threat and risk assessment.

Designated information

Subject to discretionary exceptions, mark designated documents with the PROTECTED in the upper right corner of the face of the document. In addition, the reason for the sensitivity of information marked PROTECTED or the type of safeguard required may be added. The following letters may be used to signal appropriate safeguards for designated information: "A" for low-sensitive; "B" for particularly sensitive; and "C" for extremely sensitive.

General

- Mark covering or transmittal letters or forms or circulation slips to show the highest level of classification or designation of the attachments.
- Mark all materiels used in preparing classified and designated information. Examples of such materiel include notes, drafts, and photocopies.
- Marking may also specify who may or may not access the information, in order to further limit access.
- Security markings should include the applicable classification or designation and the date or event at which declassification or downgrading is to occur; if it is possible, determine this at the time the information is created or collected.
- Assign a security classification or designation commensurate with the highest classification or designation of the information contained on a microform.
- Mark microforms containing classified information with the proper classification in eye-readable form with the microform number and the total number of microforms.
- Mark microforms containing designated information PROTECTED in eye-readable form with the microform number and the total number of microforms.
- For information on the marking of electronic storage media, see the document entitled *Technical Security Standards for Information Technology* listed in Appendix A to Chapter 2-3.