Department of Justice
Canada

Ministère de la Justice
Canada

RESPONSE
OF THE
GOVERNMENT OF CANADA
TO THE
REPORT OF THE PARLIAMENTARY SUB-COMMITTEE
ON
COMPUTER CRIME

Canada

OCTOBER, 1983

Response of the Government of Canada
to
the Request by the Standing Committee
on Justice and Legal Affairs
for
the Government to Table a
Comprehensive Response to the
Ninth Report of the Committee
Pursuant to Standing Order 69(13)
of the House of Commons

As recognized in the Report of the Sub-Committee on Computer Crime, Canadian society is evolving into an information based economy. A significant proportion of Canada's gross national product and the employment of its citizens is related to the production, processing, storage and use of information. As a result, Canadians are being challenged to devise new legal, economic and social arrangements that will ensure the creation and effective utilization of new information and technology, which will be in line with basic political and human values so as to to protect against unwise applications or restrictions of that new information and technology.

In helping Canadians to understand the complexities of the issues, the Government commends the Sub-committee on Computer Crime for its study of computer and computer related crime, and related information issues; and wishes to respond to the recommendations in the order in which they were made.

1. **The Sub-committee recommends that the Criminal Code be amended to create two new offences: the unauthorized access (without colour of right) to a computer system, and the unauthorized alteration or destruction (without colour of right) of computerized data. The Sub-committee further recommends that Crown prosecutors be given the option of proceeding either by indictment or by way of summary conviction (para.37).**

On July 25, 1983, the Minister of Justice released for public comment a package of proposals to amend the criminal law, entitled: "Proposed Act to amend the

Criminal Code, to amend an Act to amend the Criminal Code and to amend the Combines Investigation Act, the Criminal Law Amendment Act, 1977, the Customs Tariff, the Food and Drugs Act, the Narcotic Control Act and the Weights and Measures Act, to repeal certain other Acts and to make other consequential amendments". Included in these proposals are two amendments to the Criminal Code, attached as Attachment "A", to bring the criminal law up to date in respect of the protection of the integrity of computer systems.

In particular, clause 54 of the Proposed Act to amend the Criminal Code et. al. proposes that a new section be added to provide that it would be an offence to fraudulently and without colour of right (a) obtain a computer service, (b) intercept a function of a computer system or, (c) use a computer system with intent to commit any of the two previously mentioned offences or the offence of mischief in relation to data or a computer system. Clause 67 proposes that a new sub-section be added to include within the offence of mischief the wilful (a) destruction or alteration of data, (b) the rendering of data meaningless, useless or ineffective, (c) the obstruction, interruption or interference with the lawful use of data and, (d) the obstruction, interruption or interference with any person in the lawful use of data or the denial of access to data to any person who is entitled to access thereto. Both clauses 54 and 67 provide that a person who commits any of these offences is guilty of an indictable offence and is liable to imprisonment for ten years, or is guilty of an offence punishable on summary conviction.

These proposals are consistent with the recommendations of the Sub-Committee, and in many respects, afford greater protection to the integrity of computer systems. The Minister of Justice intends to introduce these proposals, or similar proposals, in the form of a Bill during this Parliament.

2. The Sub-committee recommends that the definitions necessary to the description of the substantive offences be expressed, to the greatest extent possible in terms of function rather than of technology (para. 38).

The Government agrees that any definitions utilized to assist in the description of the proposed offences be expressed conceptually, to the greatest extent possible, in terms of function, rather than be tied to present technology. On the other hand, the Government also recognizes the fundamental principle of criminal law that the definition of offences be precise and fair in order to assist in the proper interpretation of legislative provisions and to give proper notice to the public of the activities specifically prohibited. The definitions and the description of the offences in the Proposed Act to amend the Criminal Code et. al., supra, fulfill these two aims.

3. The Sub-committee recommends that a comprehensive review of all matters relating to the effective detection and prosecution of computer crime be undertaken. Special attention should be paid to the adequacy of existing powers of search and seizure, the federal acts and treaties relating to international investigations and extraditions, and the wire-tap provisions of the Criminal Code as they relate to communications between computers (para. 47).

The Department of Justice, the Ministry of the Solicitor General, the Law Reform Commission of Canada and the provincial departments of the Attorney General are currently involved in a comprehensive Review of the Criminal Law initiated by the Government in 1980. In the course of this review, the search and seizure powers and wire-tap provisions of the Criminal Code will be reviewed and attention will be directed to the problems posed by computer technology in these areas.

The Department of Justice has initiated a review of the Extradition Act and Fugitive Offenders Act, in the course of which attention will be directed to the ability to request or provide extradition in respect of computer or computer-related crimes.

In addition, Canada is a member of the Committee on Information, Computers and Communications Policy of the Organization of Economic Cooperation and Development (O.E.C.D.), and chairs the Working Party on Transborder Data Flow. Canada has recently

participated in an O.E.C.D. review of member countries' attitudes, approaches and policies to computer and computer-related crime.

On November 18, 1982, the Government introduced, in the Senate, Bill S-33, a proposed new Canada Evidence Act. Included in the Bill are provisions relevant to the admissibility in judicial proceedings of computer print-outs and other computer generated evidence. Second Reading of the Bill occurred on December 7, 1982, and on June 28, 1983, the Standing Committee on Legal and Constitutional Affairs issued an Interim Report. Pursuant to the Report, the Department of Justice is conducting consultations with the provincial Attorneys General, the Canadian Bar Association and other interested groups and individuals with a view to introducing an amended version of the Bill.

4. The Sub-committee recommends that every effort be made to ensure that law enforcement agents and prosecutors who are likely to deal with cases involving computer crime receive the necessary computer training to carry out their functions effectively (para. 48).

Since June of 1980, the Canadian Police College in Ottawa has held nine Computer Crime Investigation Techniques Courses designed and co-ordinated by the R.C.M.P. A total of 180 candidates, 109 R.C.M.P. and 71 from other police departments, have been trained. This course, is specifically for experienced white collar crime investigators with no previous computer experience. The course prepares the candidates to investigate criminal offences involving computers by making them familiar with the computer environment in order to enable them to identify the potential avenues of investigation.

The course is divided into five major areas: Computers and Electronic Data Processing Fundamentals, Introduction to Computer Programming, Computer Security, The Law and Evidence, and Computer Crime. The first segment is designed to remove the mystique that surrounds the computer as viewed by the environment and data processing personnel. The next segment provides instruction in computer language and

programming. The Computer Security segment deals with the concept of computer security, security systems and their vulnerabilities. The last two segments, The Law and Evidence, and Computer Crime, are closely interrelated. Case studies involving fictitious business concerns require the candidate to investigate offences of theft and fraud, paying particular attention to potential suspects, systems vulnerabilities, and objects of evidence for court purposes. These sessions also include analysis of notable national and international cases. The course is constantly being monitored and amended to reflect changes in the computer environment.

The primary responsibility for the enforcement and prosecution of the criminal law lies with the provincial Attorneys General. The Government is, therefore, unable to comment on the existence or extent of training for provincial and municipal police forces or provincial prosecutors, except to state that some training of provincial and municipal police officers is available through the Canadian Police College.

5. The Sub-committee recommends that the computer industry and institutional users recognize the potential for computer crime and adopt appropriate security measures (para. 51).

The EDP Security Evaluation and Inspection Team (SEIT), organized and administered by the R.C.M.P., is responsible for conducting inspections and evaluations of government EDP facilities as well as private sector facilities engaged in processing government information under contract.

The following documentation is attached, as Attachment 'B': Excerpts from Treasury Board Administrative Policy Manual on EDP Security; and Schedules A, B and C of the Financial Administration Act. These documents describe, in some detail, the involvement of the Government in this important area.

6. The Sub-committee recommends that the Copyright Act be amended to include computer software (para. 55).

The Ministers of Consumer and Corporate Affairs and Communications are considering revisions to the Copyright Act including measures dealing with computer software.

7. The Sub-committee recommends that the federal government undertake a comprehensive study to examine the feasibility of extending patent and industrial design protection to computer programs (para. 56).

The issue of the protection of intellectual property in respect of computer software is currently being studied by the Department of Consumer and Corporate Affairs.

8. The Sub-committee recommends that both levels of government undertake a comprehensive joint study of trade secrecy law and adopt corrective measures (para. 58)

The Government wishes to note that the issues involved in the protection of information are not solely related to computer usage. In June, 1983, the Department of Justice, in conjunction with the Alberta Institute of Law Research and Reform, completed a preliminary study of the need for the development in Canada of uniform civil law protection for trade secrets and other types of confidential commercial information, as well as criminal law sanctions consistent with such protection. In line with the recommendation of the Sub-Committee, the Government proposes to discuss with the provinces the possibility of establishing a federal-provincial study to consider the type of protection which the law should recognize in these areas.

The Committee's report (at paragraphs 59-62) includes only a partial reference to federal legislation which provides for the protection of personal information held by the federal public sector. As a matter of clarification, the Government

would like to indicate that the Privacy Act, S.C. 1980-81-82-83, c.111, contains a comprehensive code regulating the use and disclosure of personal information held by federal government institutions (sections 7 and 8). These provisions are very similar to those included in the new Quebec legislation on access to public documents and the protection of personal information which the Committee specifically commends. In addition, there are provisions requiring the confidential handling of information by the federal government in over fifty-three statutes. Many of these deal with personal information, while others deal with confidential commercial information.

9. The Sub-committee recommends that the computer industry ensure, through self-regulation, a high standard of conduct in the industry (para. 65).

The Government is supportive of efforts by the computer industry to set high ethical standards in the use of computer systems and to utilize appropriate security measures. The R.C.M.P. assists in this area through the work of the Security Evaluation and Inspection Team. It also pursues an EDP security awareness programme through the publication of literature concerning computer security.

10. The Sub-committee recommends that knowledge of computer ethics be a qualification for educators involved in teaching computer skills and that the ethics of computer use be integrated into computer classes at all levels. (para. 67).

Education is largely a responsibility of the provincial legislatures. The Government is, however, active in this area, through the R.C.M.P., by providing EDP security training at the Canadian Police College in Ottawa. Computer ethics is an integral part of this training.The Government is also considering the introduction of a computer ethics segment into the professional development courses on operation of computers, which are sponsored by the Public Service Commission.

Minister of Justice
The Honourable
Mark MacGuigan

Ministre de la Justice
L'honorable
Mark MacGuigan

Proposed Act to amend the Criminal Code, to amend an Act to amend the Criminal Code and to amend the Combines Investigation Act, the Criminal Law Amendment Act, 1977, the Customs Tariff, the Food and Drugs Act, the Narcotic Control Act and the Weights and Measures Act, to repeal certain other Acts and to make other consequential amendments

Ottawa, Canada
K1A 0M8

25516-11-7-83

54. The said Act is further amended by adding thereto, immediately after section 301.1 thereof, the following section:

Unauthorized use of computer

"**301.2** (1) Every one who, fraudulently and without colour of right,

(*a*) obtains, directly or indirectly, any computer service,

(*b*) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or

(*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 387 in relation to data or a computer system

is guilty of an indictable offence and is liable to imprisonment for ten years, or is guilty of an offence punishable on summary conviction.

Interpretation

(2) In this section,

"computer program" «*programme d'ordinateur*»

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" «*service d'ordinateur*»

"computer service" includes data processing and the storage or retrieval of data;

"computer system" «*ordinateur*»

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(*a*) contains computer programs or other data, and

(*b*) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"data" «*donnée*»

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electromagnetic, acoustic, mechanical or other device" «*dispositif électromagnétique*»

"electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" «*fonction*»

"function" includes logic, control, arithmetic, communication, storage and retrieval;

"intercept" «*intercepter*»

"intercept" has the same meaning as in section 178.1."

67. (1) Section 387 of the said Act is amended by adding thereto, immediately after subsection (1) thereof, the following subsection:

"(1.1) Every one commits mischief who wilfully

(*a*) destroys or alters data;

(*b*) renders data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use of data; or

(*d*) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto."

1972, c. 13, s. 30

(2) Subsections 387(3) to (5) of the said Act are repealed and the following substituted therefor:

Idem

"(3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds five hundred dollars

(*a*) is guilty of an indictable offence and is liable to imprisonment for ten years; or

(*b*) is guilty of an offence punishable on summary conviction.

Idem

(4) Every one who commits mischief in relation to property, other than property described in subsection (3),

(*a*) is guilty of an indictable offence and is liable to imprisonment for two years; or

(*b*) is guilty of an offence punishable on summary conviction.

Idem

(5) Everyone who commits mischief in relation to data

(*a*) is guilty of an indictable offence and is liable to imprisonment for ten years; or

(*b*) is guilty of an offence punishable on summary conviction.

Offence

(5.1) Every one who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,

(*a*) is guilty of an indictable offence and is liable to imprisonment for five years; or

(*b*) is guilty of an offence punishable on summary conviction."

(3) Section 387 is further amended by adding thereto the following subsection:

Definition of data

"(8) In this section, "data" has the same meaning as in section 301.2."

Administrative policy manual

Chapter 440, Section 8

EDP: security

December 1978

Table of contents

Key definitions

Directives: statements indicating mandatory features of a policy. In those cases where Treasury Board is prepared to permit deviations, departments must obtain prior approval by means of submissions. Directives are characterized by the use of the verbs *shall*, *must* and *will*, and appear in ***bold italics***.

Guidelines: statements indicating instructions which, while not mandatory, should be followed unless there is good reason not to do so. While valid reasons for non-compliance must be documented, prior Treasury Board approval is not required. Guidelines are characterized by the use of the verb *should*, and appear in *italics*.

.8.1 Purpose and scope

Deputy heads of departments and heads of agencies are responsible for establishing appropriate security measures within the departments and agencies of government. The purpose of this section is to provide guidance in the exercise of these responsibilities within the electronic data processing (EDP) environment. It is intended to assist those with responsibility for the planning of security and the development of security procedures in an EDP environment.

Impenetrable security is generally thought to be unattainable. An optimum security system is one in which the cost of providing the security against a given threat in a given period has been balanced against the probability of the security infraction occurring and the consequences, financial or otherwise, to the government if it does. This kind of balance should be achieved for all differing threats to which information, personnel, or property can be subjected.

In most situations, particularly those in which governments find themselves, it is extremely difficult to determine either the probability of occurrence of a given threat, or the cost involved if the threat becomes a fact. Nonetheless, the importance of evaluating the possible threats and their impact before deciding what security measures are appropriate in any particular EDP environment cannot be overemphasized. In most cases it is possible to evaluate, within a factor of ten, both the expected frequency of occurrence and the cost associated with any defined threat. This will at least provide guidance on the appropriate emphasis of the security system.

Security threats depend greatly on the type of information being handled. Information which is being sought by a foreign power clearly warrants different protective measures from information which may be sought by a private citizen about a neighbour. Continuity of computer service is clearly more critical in support of some processes than for others. It is certain, however, that all data processing resources are worthy of at least a minimum level of protection. This section addresses the problem of minimum security standards and is therefore applicable to every data processing situation in government. In this respect, some departments need to impose more stringent rules than those contained herein.

Many aspects of security in an EDP environment are common to security in other environments. For these aspects established procedures and practices generally exist separately; such aspects are only briefly mentioned herein because guidance is readily available from departmental

security officers and government agencies with specific security responsibilities.

.8.2 Application

This section was prepared with the assistance and concurrence of the Security Advisory Committee. It applies to agencies named in Schedule C of the *Financial Administration Act*, as well as to departments and agencies named in Schedules A and B, and to branches designated as departments for purposes of the Act. The provisions of this chapter will not apply to the Department of National Defence when inconsistent with the organization and operational needs of that department as prescribed under the authority of the *National Defence Act*.

.8.3 Roles and responsibilities

A number of organizations and entities have responsibility for various aspects of security in the government of Canada. Many of the security responsibilities indicated below are not specific to EDP, but are listed here for reader convenience. This list is included only to serve as a quick reference, not as an authoritative source.

.8.3.1 *Deputy ministers and heads of agencies* are solely responsible for the implementation and administration, within their department or agency, of government security policies and procedures as set out in references (a) and (b) of article .8.7. This includes responsibility for determining the level of security required by EDP services employed to process the work of their departments and agencies.

.8.3.2 *The departmental security officer (DSO)* is responsible to the deputy minister or head of agency for ensuring the implementation, coordination, supervision and audit of all security policies, standards and procedures, including those that affect EDP within his department.

.8.3.3 *The Security Advisory Committee (SAC)* is an interdepartmental body which provides advice on security matters, and counsel and guidance for the resolution of security-related conflicts within the government.

.8.3.4 *The Interdepartmental Computer Security Panel (ICSP)* is an advisory body reporting to the SAC and consisting of representation from selected government centres of EDP. It is responsible for making recommendations and providing advice on security issues relating to EDP practices and for

reviewing and advising on the activities of the EDP Security Evaluation and Inspection Team.

.8.3.5 ***The Communications - Electronic Security Committee (CSC)*** is an interdepartmental advisory body reporting to the SAC on the security of government communications.

.8.3.6 ***The Security Equipment Advisory Committee (SEAC)*** is an interdepartmental committee reporting to the SAC and is responsible for all matters relating to the provision of approved physical security equipment for government use.

.8.3.7 ***The Commissioner, Royal Canadian Mounted Police (RCMP),*** is responsible for advising deputy ministers and heads of agencies on the implementation of government security policies as outlined in directives, regulations and instructions, consistent with responsibilities allocated in these directives and guidelines. He may obtain assistance for certain aspects of this responsibility from other departments and agencies within government as mutually agreed upon.

The Commissioner, RCMP, is responsible for the organization and operation of the EDP Security Evaluation and Inspection Team.

.8.3.8 ***The EDP Security Evaluation and Inspection Team (SEIT),*** organized and administered by the RCMP in accordance with the provisions of this section, and drawing upon interdepartmental resources when practical, is responsible for conducting inspections and evaluations of government EDP facilities as well as private sector facilities engaged in processing government information under contract.

.8.3.9 ***The Department of Supply and Services (DSS)*** is responsible for the supply of, and contractual agreements for, all EDP equipment and services to be used by government departments and agencies. This includes ensuring that suppliers of equipment have incorporated into the manufacture and design of any equipment all security specifications established by government security regulations and guidelines. DSS is also responsible for arranging for the security clearance of private sector facilities and personnel, and for arranging the SEIT inspections of private sector EDP facilities.

.8.3.10 ***The Communications Security Establishment (CSE)*** the Department of National Defence has been designated as the national COMSEC agency and, as such, is responsible for the provision of guidance and advice on communications-

electronic security (COMSEC) matters to all departments and agencies of the government. The Departments of External Affairs, National Defence, Communications, Supply and Services, and Transport, as well as the Royal Canadian Mounted Police and the Privy Council Office, will deal directly with CSE on COMSEC matters. All other departments and agencies will follow the procedures set out in article .8.3.11 below.

.8.3.11 *The Department of Communications (DOC)* is responsible for providing guidance and advice on COMSEC matters to all departments and agencies not represented on the CSC. In addition, with respect to all departments and agencies, the DOC is responsible for providing other services within the intent of Chapter 430 on Telecommunications.

.8.3.12 *The Department of Public Works (DPW),* whenever it is responsible for the construction of, or structual changes to, a building, is also responsible for implementing structural requirements dictated by security standards. This includes application of the federal, provincial or municipal building codes and fire regulations, and consultation with the RCMP as to their effect on security requirements.

.8.4 **Directives**

.8.4.1 ***General security responsibilities and procedures in the EDP environment shall be those stated in the relevant departmental security manuals unless otherwise specified in these directives and guidelines.***

.8.4.2 ***Departments and agencies using EDP facilities must ensure that:***

(a) information is classified or categorized in accordance with established procedures, and circumstances are specified under which data may be downgraded or declassified; and

(b) all EDP facilities processing government information, including those under contract to the department or agency, meet specified security requirements.

.8.4.3 ***Departments and agencies using EDP facilities, either government or private sector, which are engaged in handling information for the government must ensure that:***

(a) information in their custody, in whatever form, is protected to the level required by the relevant security classifica-

tion or category and any accompanying caveats; and

(b) an EDP security threat assessment is completed and an up-to-date threat evaluation report is prepared and maintained describing potential security risks of which account has been taken.

.8.4.4 *Any government organization planning the establishment, procurement, modification or relocation of a general purpose EDP facility, system or service shall contact the departmental security officer (DSO) during the planning phase to ensure that all appropriate security authorities are consulted.*

.8.4.5 *Departments and agencies must consult with the interdepartmental Security Evaluation and Inspection Team (SEIT) regarding the security status of their EDP facilities.* Departments and agencies which have, or contemplate having, contracts that involve the processing of classified or otherwise sensitive information at a private sector EDP facility must contact the Security Branch of the Department of Supply and Services, who arrange for the SEIT to inspect the facility and provide a security evaluation report.

.8.4.6 *Departments and agencies shall advise the SEIT of the plan of action to deal with, and progress made against, outstanding problem areas identified in the report within six months of the receipt of a security evaluation report.* These progress reports shall be provided to the SEIT annually thereafter until all the recommendations have been addressed, or a reinspection has been initiated.

.8.4.7 *The RCMP will compile an annual report to the Administrative Policy Branch, Treasury Board Secretariat, on the security status of all EDP facilities serving the government.* This report will be based on the results of all previous SEIT activities, and will take into account progress reported by departments and agencies during the reporting year

.8.5 Guidelines

.8.5.1 *All directors of EDP should designate an EDP security coordinator,* who will receive direction from the DSO on security policy and report to the director of EDP on matters affecting EDP security. The security coordinator should be a senior staff member experienced in the EDP field, whose normal responsibilities require an under-

standing of EDP operations from both a management and a systems point of view. This individual should also have a general knowledge of security principles, procedures and problems.

.8.5.2 *The responsibilities of the EDP security coordinator should include*:

(a) conducting regular security threat assessments and preparing evaluation reports,

(b) developing EDP security procedures, proposals for threat counter-measures and contingency plans,

(c) periodically reviewing EDP security precautions and contingency plans,

(d) alerting the director of EDP to potential security problems, and

(e) educating and motivating EDP personnel to observe security precautions.

.8.5.3 *The EDP security evaluation report should be updated by the EDP security coordinator at annual intervals* (or more frequently if occasion demands) and should provide the basis for modifications or additions to security measures affecting EDP activities.

.8.5.4 *The interconnection of EDP systems and telecommunications services should be carefully planned and coordinated* to ensure that security of the information being processed and transmitted is provided. Advice in this regard should be requested from the appropriate authorities as indicated under articles .8.3.10 and .8.3.11.

.8.5.5 *All security criteria pertinent to an EDP job intended to be contracted should be included in any bid solicitation.* Bidders should be evaluated on their responsiveness to the specified requirements.

.8.5.6 *The originator of the data to be processed should determine and clearly indicate the security classification or category of such data.* The security marking of computer output is the joint responsibility of the originator and the EDP facility. The originator should ensure that the EDP facility manager is aware of the security requirements of the output. The EDP facility manager is responsible for the labelling and protection of the computer output as instructed by the originator.

.8.5.7 *Control measures for data input, processing, storage and output, program generation and maintenance, and hardware operation and support*

should be clearly identified in the standard operating procedures of the EDP facility.

.8.6 **Interpretation and advice**

It is the responsibility of the Security Evaluation and Inspection Team of the RCMP to evaluate the status of security in government EDP operations. This they do through regular inspections of the facilities used by the various departments and agencies. The frequency of inspection of a given facility depends on the sensitivity of the data and information processed, and how critical the service provided is in relation to overall government objectives and priorities.

Following inspection of a facility, the SEIT will prepare an evaluation report for the deputy head in charge of the facility indicating the classification level or category of information which SEIT considers the facility can handle and process securely. Copies of the evaluation report will also be provided to the DSO, and the responsible director(s) of EDP.

In the case of private sector facilities under contract, an evaluation report will be provided for the Director, Security Branch, DSS who will subsequently make the results available to the chief officer of the private sector organization. These results are made available by DSS on request, to departments and agencies contracting for EDP services from the subject facility.

Copies of all SEIT reports will be made available on request, to the Administrative Policy Branch, Treasury Board Secretariat, and the Chairman, Security Advisory Committee.

Within sixty days of delivery of a security evaluation report, the SEIT will contact the DSO of the subject department or agency to provide [illegible]tation and advice on observations and [illegible]endations as necessary. This should lead to the formulation of an action plan on the part of [illegible]ility management and security personnel to address outstanding security problems and recommendations of the report.

The rating criteria used for EDP security evaluations are the EDP Security Standards prepared under the direction of the ICSP, and in consultation with the Government EDP Standards Committee.

.8.7 **References**

- *Official Secrets Act* (RSC 1970, Chapter 0-3).
- Chapter 430, Telecommunications.

FINANCIAL ADMINISTRATION

Schedule A

Department of Agriculture
Department of Communications
Department of Consumer and Corporate Affairs
Department of Employment and Immigration
Department of Energy, Mines and Resources
Department of the Environment
Department of External Affairs
Department of Finance
Department of Fisheries and Oceans
Department of Indian Affairs and Northern Development
Department of Industry, Trade and Commerce
Department of Insurance
Department of Justice
Department of Labour
Department of National Defence
Department of National Health and Welfare

Department of National Revenue
Department of Public Works
Department of Regional Economic Expansion
Department of Supply and Services
Department of the Secretary of State of Canada
Department of the Solicitor General
Department of Transport
Treasury Board
Department of Veterans Affairs
1960, c. 41, s. 16; 1963, c. 3, s. 18; 1966-67, c. 25, s. 33; 1967-68, c. 16, s. 13, 1968-69, c. 27, s. 20.

Schedule B

Agricultural Stabilization Board
Atomic Energy Control Board
Canada Employment and Immigration Commission

Director of Soldier Settlement
The Director, The Veterans' Land Act

Economic Council of Canada
Fisheries Prices Support Board
Medical Research Council of Canada
Municipal Development and Loan Board

National Museums of Canada
National Research Council of Canada
Natural Sciences and Engineering Research Council

Science Council of Canada
Social Sciences and Humanities Research Council
RS, c. 116, Sch. B; 1957-58, c. 22, s. 15; SOR/63-430, 431; SOR/68-151; SOR/69-257, 305.

Schedule C

Atomic Energy of Canada
Canada Harbours Place Corporation
Canada Museums Construction Corporation Inc.

Schedule C (cont'd)

Canada Post Corporation
Canada Lands Company Limited
Canada Lands Company (Mirabel) Limited
Canada Lands Company (Le Vieux Port de Montréal) Limited
Canada Lands Company (Vieux-Port de Québec) Inc.

Canadian Arsenals Limited
Canadian Commercial Corporation
Canadian Dairy Commission
Canadian Film Development Corporation

Canadian Livestock Feed Board
Canadian National (West Indies) Steamships, Limited
Canadian Patents and Development Limited

Canadian Saltfish Corporation
Crown Assets Disposal Corporation

Defence Construction (1951) Limited
Loto Canada Inc.
National Battlefields Commission
National Capital Commission
National Harbours Board
Northern Canada Power Commission

Public Works Lands Company Limited
Royal Canadian Mint
Uranium Canada Limited
RS, c. 116, Sch. C; SOR Con. 1955 Vol. 2, p. 1400; SOR/55-224; PC 1960-1684; SOR/63-72; SOR/66-559; SOR/67-230; SOR/68-68; SOR/69-270.