JAN 19 1984

ANNEX A CONFIDENTIAL

AN OPERATIONAL POLICY FOR THE PROTECTION OF GOVERNMENT OF CANADA ASSETS

T A B L E O F C O N T E N T S

AN OPERATIONAL POLICY FOR THE PROTECTION OF GOVERNMENT OF CANADA ASSETS

PURPOSE

Purpose

1. This paper provides operational policy regarding all aspects of the protection of government assets which affect the national interest or the public interest. This operational policy will serve as the framework for the formulation of directives and guidelines governing the essential components of a security program for government institutions.

DEFINITIONS

Definitions

2. In this operational policy,

"administration of security" means that component of security which involves the establishment and management of a security organization within government institutions and the development and implementation of a security program;

"approved" means approved by the Treasury Board, or in a manner approved by Treasury Board;

"asset" means any information or material owned by or in the custody or control of the Government of Canada;

"basic physical security" means security for the fabric of the building, external landscaping and for those parts commonly used by more than one department or agency and for those parts normally available to the public;

"classified" means assigned a designation of TOP SECRET, SECRET, CONFIDENTIAL, PROTECTED-1 or PROTECTED-2;

"communications-electronic security (COMSEC)" means that component of security which involves the use of specialized technical and physical security measures to protect classified information transmitted by electrical means and certain electronic emissions associated with classified activities;

"construction" means the fabrication of permanent elements of a building, including the approaches, external landscaping, and entrances and exits;

"Council" means the Queen's Privy Council for Canada, committees of the Queen's Privy Council for Canada, Cabinet and committees of Cabinet;

"cryptographic system" means a system which renders plain text unintelligible, through encryption, and reconverts encrypted information into intelligible form;

"defence establishment" means any area or structure under the control of the Minister of National Defence, and the material and other things situated in or on any such area or structure;

"defence of Canada or any state allied or associated with Canada" includes the efforts of Canada and of foreign states toward the detection, prevention or suppression of activities of any foreign state directed toward actual or potential attack or other acts of aggression against Canada or any state allied or associated with Canada;

"deputy head" means, in relation to

i) a department named in Schedule A to the Financial Administration Act, the deputy minister thereof,

ii) the Canadian Forces, the Chief of Defence Staff,

iii) the Royal Canadian Mounted Police, the Commissioner, and

iv) any other portion of the Public Service, the person designated by Order-in-Council to be the deputy head of that portion of the Public Service;

"electronic data processing (EDP) security" means that component of security which involves the use of hardware equipment, software systems and operating procedures to protect classified information processed by EDP systems;

"emission security" means measures taken to deny unauthorized persons information of value which might be derived from the interception and analysis of undesired emanations from equipment used to process classified information;

"fabric of the building" means the permanent elements of the building structure including electrical/mechanical systems, entrances, exits and approaches;

"field investigation" means inquiries, such as interviews of references and other individuals, to assist in determining the suitability of a person for a security clearance;

"government" means the Government of Canada;

"government institution" means any Government of Canada department, ministry of state, body or office identified by paragraph 3 of this policy;

"information" means any pattern of symbols or sounds to which meaning may be assigned;

"investigative body" means any government institution, or part of a government institution, that is specified as such in Schedule 1 of the Regulations passed pursuant to the Access to Information Act;

"material" means any tangible object, excluding information;

"multiple occupancy building" means a building occupied by two or more government institutions neither/none of which occupies 75 per cent or more of the space;

"national interest" means matters referred to in the Access to Information Act under the exemptable classes of information relating to the fundamental safety and integrity of Canada including: defence against armed attack by another state, or against subversive and hostile activities; the conduct of international and federal-provincial affairs; management of the national economy; the confidentiality of Cabinet activities; and, ministerial advice relating to the above concerns;

"personal information" means information defined as personal information in section 3 (a) to (i) of the Privacy Act;

"personnel security" means the development and implementation of policy and procedures related to the suitability of persons who will have access to classified assets;

"physical security" means that component of security which involves the development and implementation of policy and procedures to physically deny, or control, access to classified assets of the Federal Government;

"physical security equipment" means equipments, installations and building components designed or used to physically deny, or control, access to classified assets of the government, and includes such ancillary systems as are vital to the proper operation of those equipments, installations and building components;

"position description" means the written explanation of the functions, objectives, responsibilities, accountability and security classification level requirement of a position, or class of positions;

"public interest" means matters referred to in the Access to Information Act and the Privacy Act under the classes of exemptable information relating to the privacy, safety, financial and proprietary interests of individuals, groups and organizations; the competitiveness of private commercial interests; law enforcement and the administration of justice; and, except where such matters have a direct and material impact

upon the national interest, information provided to the government in confidence by an international organization of states or an institution thereof, the government of a province or an institution thereof, or a municipal or regional government or an institution of such government and ministerial advice relating to all of the above;

"security clearance" means a finding, based on a security assessment, that an individual has satisfied the security requirements of the position in question;

"single occupancy building" means a building 75 per cent or more of which is occupied by one government institution;

"statement of qualifications" means a written specification of the essential and desirable qualifications pertinent to the staffing of a position or group of positions;

"subversive or hostile activities" means FROM PRIVACY & A.T.I. ACTS

i) espionage against Canada or any state allied or associated with Canada,

ii) sabotage,

iii) activities directed toward the commission of terrorist acts, including highjacking, in or against Canada or foreign states,

iv) activities directed toward accomplishing government change within Canada or foreign states by the use of or the encouragement of the use of force, violence or any criminal means,

v) activities directed toward gathering information used for intelligence purposes that relates to Canada or any state allied or associated with Canada, and

vi) activities directed toward threatening the safety of Canadians, employees of the Government of Canada or property of the Government of Canada outside Canada.

"supporting utilities and services" means the electrical power, heating, air conditioning, water, cleaning, maintenance, transportation, fire protection and waste disposal utilities and services which are provided to facilities or equipment;

"technical intrusion security" means that component of security which protects against audio, visual, optical and/or electronic techniques, excepting emission security, which could compromise the security of a given area.

"telecommunications" means any transmission, emission or reception of signs, signals,

writing, images, sound or intelligence of any nature by wire, radio, visual or other electromagnetic system.

APPLICATION

Application

3. This operational policy applies to the government institutions listed in Schedule I of Access to Information Act (1982) as amended from time to time, and to other government institutions that may be designated by the President of the Treasury Board.

CLASSIFICATION AND PROTECTION OF ASSETS

Classification

4. Information and material assets of the Government of Canada the unauthorized disclosure, destruction, removal, modification or interruption, of which would be injurious to either the national interest or the public interest shall be identified by a system of classification for special protection. Such classification and measures of protection shall be administered in accordance with directives and guidelines issued pursuant to this operational policy.

ASSETS AFFECTING THE NATIONAL INTEREST

Information Assets

5. The following government information shall be considered for classification in the national interest:

Information obtained in confidence

a) information that was obtained in confidence from:

i) the government of a foreign state or an institution thereof;

ii) an international organization of states or an institution thereof, when the information relates to a class of information in b), c) or d) below;

iii) the government of a province or an institution thereof, when the information relates to a class of information in b), c) or d) below;

iv) a municipal or regional government established by an Act of the legislature of a province or an institution of such a government, when the information relates to a class of information in b), c) or d) below.

Federal-provincial affairs

b) information on the conduct by the Government of Canada of federal-provincial affairs, including, without restricting the generality of the foregoing:

i) information on federal-provincial consultations or deliberations, and

ii) information on strategy or tactics adopted or to be adopted by the

Government of Canada relating to the conduct of federal-provincial affairs.

International affairs and defence

c) information on 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, including, without restricting the generality of the foregoing:

i) information relating to military tactics or strategy, or information relating to military exercises or operations undertaken in preparation for hostilities or in connection with the detection, prevention or suppression of subversive or hostile activities;

ii) information relating to the quantity, characteristics, capabilities or deployment of weapons or other defence equipment or of anything being designed, developed, produced or considered for use as weapons or other defence equipment;

iii) information relating to the characteristics, capabilities, performance, potential, deployment, functions or role of any defence establishment, of any military force, unit or personnel or of any organization or person responsible for the detection, prevention or suppression of subversive or hostile activities;

iv) information obtained or prepared for the purpose of intelligence relating to:

(A) the defence of Canada or any state allied or associated with Canada, or

(B) the detection, prevention or suppression of subversive or hostile activities;

v) information obtained or prepared for the purpose of intelligence respecting foreign states, international organizations of states or citizens of foreign states used by the Government of Canada in the process of deliberation and consultation or in the conduct of international affairs;

vi) information on methods of, and scientific or technical equipment for collecting, assessing or handling information referred to in 5 c)iv) or v) above and information on sources of such information;

vii) information on the positions adopted or to be adopted by the Government of Canada, governments of foreign states or international organizations of states for the purpose of present or future international negotiations;

viii) diplomatic correspondence exchanged with foreign states or international organizations of states or official correspondence exchanged with Canadian diplomatic missions or consular posts abroad, and

ix) information relating to the communications or cryptographic systems of Canada or foreign states used:

(A) for the conduct of international affairs,

(B) for the defence of Canada or any state allied or associated with Canada, or

(C) in relation to the detection, prevention or suppression of subversive or hostile activities.

Economic interests of Canada

d) i) information which relates to:

(A) trade secrets or financial, commercial, scientific or technical information that belongs to the Government of Canada or a government institution and has substantial value or is reasonably likely to have substantial value; or

(B) information on the financial interests of the Government of Canada or the ability of the Government of Canada to manage the economy of Canada including, without restricting the generality of the foregoing, any such information relating to

(1) the currency, coinage or legal tender of Canada,

(2) a contemplated change in the rate of bank interest or in government borrowing,

(3) a contemplated change in tariff rates, taxes, duties or any other revenue source,

(4) a contemplated change in the conditions of operation of financial institutions,

(5) a contemplated sale or purchase of securities or of foreign or Canadian currency, or

(6) a contemplated sale or acquisition of land or property.

Memoranda to Cabinet, discussion papers and other Cabinet documents

e) i) information that falls within any of the following classes:

(A) memoranda the purpose of which is to present proposals or recommendations to Council;

(B) discussion papers the purpose of which is to present background explanations, analyses or problems or policy options to Council for consideration by Council in making decisions;

(C) agendas of Council or records recording deliberations or decisions of Council;

(D) records used for or reflecting communications or discussions between Ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy;

(E) records the purpose of which is to brief Ministers of the Crown in relation to matters that are before, or are proposed to be brought before, Council or that are the subject of communications or discussions referred to in e)i)(D) above, or

(F) draft legislation.

Records containing information about Cabinet

ii) information about the contents of any record within a class of records referred to in e)i) above.

Advice, etc.

f) information, relating to the contents of 5 a) to 5 d) above, that falls within any of the following classes:

i) advice or recommendations developed by or for a government institution or a Minister of the Crown;

ii) an account of consultations or deliberations involving officials or employees of a government institution, a Minister of the Crown or the staff of a Minister of the Crown;

iii) positions or plans developed for the purpose of negotiations carried on or

to be carried on by or on behalf of, the Government of Canada and considerations relating thereto, or

iv) plans relating to the management of personnel or the administration of a government institution that have not yet been put into operation.

Statutory prohibitions against disclosure

g) information relating to the contents of 5 a) to 5 d) above, the disclosure of which is restricted by or pursuant to any provision set out in Schedule II of the Access to Information Act.

6. When it is determined that information falls within the general category of information relating to the national interest, it shall be designated as TOP SECRET, SECRET or CONFIDENTIAL according to the following criteria:

a) Government information shall be designated as TOP SECRET when unauthorized disclosure, destruction, removal, modification or interruption could reasonably be expected to cause exceptionally grave injury to the national interest of Canada;

b) Government information shall be designated as SECRET when unauthorized disclosure, destruction, removal, modification or interruption could reasonably be expected to cause serious injury to the national interest of Canada; or

c) Government information shall be designated as CONFIDENTIAL when unauthorized disclosure, destruction, removal, modification or interruption could reasonably be expected to cause injury to the national interest of Canada.

Material Assets

7. Government material assets shall be designated as TOP SECRET, SECRET or CONFIDENTIAL when unauthorized access to the material asset could reasonably be expected to cause injury to the national interest through the unauthorized disclosure of information, designated as TOP SECRET, SECRET or CONFIDENTIAL.

8. When unauthorized access to government material assets could reasonably be expected to cause injury to the national interest, through the destruction, removal, modification or interruption of materials or services essential to those matters to which information classified in the national interest relates, appropriate protective measures shall be considered, including where practicable, classification.

9. The specific designations shall be determined on the same basis of injury as are those for information as described in paragraph 6.

ASSETS AFFECTING THE PUBLIC INTEREST

Information Assets

10. The following government information shall be considered for classification in the public interest:

Law Enforcement and Investigations

a) i) information obtained or prepared by any government institution or part of a government institution that is an investigative body in the course of investigations pertaining to:

(A) the detection, prevention or suppression of crime, or

(B) the enforcement of any law of Canada or a province;

ii) information relating to investigative techniques or plans for specific lawful investigations;

iii) information, on the enforcement of any law of Canada or a province or the conduct of lawful investigations as defined in Section 16(4) of the Access to Information Act and in Schedule II of the Regulations passed pursuant to that Act, including, without restricting the generality of the foregoing, any such information

A) relating to the existence or nature of a particular investigation,

B) that would reveal the identity of a confidential source of information, or

C) that was obtained or prepared in the course of an investigation; or

iv) information on the security of penal institutions.

Security

b) information which could facilitate the commission of an offence, including, without restricting the generality of the foregoing:

i) information on criminal methods and techniques;

ii) technical information relating to weapons or potential weapons, and

iii) information on the vulnerability of particular buildings or other structures or systems including computer or communication systems, or methods employed to protect such buildings or other structures or systems.

icing services for provinces or municipalities

c) information that was obtained or prepared by the Royal Canadian Mounted Police while performing policing services for a province or a municipality pursuant to an arrangement made under section 20 of the Royal Canadian Mounted Police Act, where the Government of Canada has, on the request of the province or the municipality, agreed to protect such information.

Safety of individuals

d) information which could threaten the safety of individuals.

Private financial or proprietary interests

e) i) information that includes:

(A) information which could result in an undue benefit to any person, including, without restricting the generality of the foregoing, any such information relating to

(1) the currency, coinage or legal tender of Canada,

(2) a contemplated change in the rate of bank interest or in government borrowing,

(3) a contemplated change in tariff rates, taxes, duties or any other revenue source,

(4) a contemplated change in the conditions of operation of financial institutions,

(5) a contemplated sale or purchase of securities or of foreign or Canadian currency, or

(6) a contemplated sale or acquisition of land or property.

ii) information on the competitive position of a government institution;

iii) scientific or technical information obtained through research by an officer or employee of a government institution.

Personal information

f) personal information.

Third party information

g) information containing:

i) trade secrets of a third party;

ii) financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party and is treated consistently in a

confidential manner by the third party;

iii) information on the competitive position of, a third party, or

iv) information on contractual or other negotiations of a third party.

Product or environmental testing

h) information containing the results of product or environmental testing carried out by or on behalf of a government institution if:

i) the testing was done as a service to a person, a group of persons or an organization other than a government institution and for a fee, or

ii) the information is the results of preliminary testing conducted for the purpose of developing methods of testing.

Testing procedures, tests and audits

i) information relating to testing or auditing procedures or techniques or details of specific tests to be given or audits to be conducted.

Solicitor-client privilege

j) information that is subject to solicitor-client privilege.

Security Clearances

k) any personal information that was obtained or prepared by an investigative body for the purpose of determining whether to grant security clearances:

i) required by the Government of Canada in respect of individuals employed by or performing services for the Government of Canada or a government institution, individuals employed by or performing services for a person or body performing services for the Government of Canada or individuals seeking to be so employed or seeking to perform such services; or

ii) required by the government of a province or a foreign state or an institution thereof.

Advice, etc.

l) information, relating to the contents of 10 a) to 10 k) above, that falls within any of the following classes:

i) advice or recommendations developed by or for a government institution or a Minister of the Crown;

ii) an account of consultations or deliberations involving officials or employees of a government institution, a Minister of the Crown or the staff of a Minister of the Crown;

iii) positions or plans developed for the purpose of negotiations carried on or to be carried on by or on behalf of the Government of Canada and considerations relating thereto, or

iv) plans relating to the management of personnel or the administration of a government institution that have not yet been put into operation.

Statutory prohibitions against disclosure

m) information, relating to the contents of 10 (a) to 10 (k) above, that contains information, the disclosure of which is restricted by or pursuant to any provision set out in Schedule II of the Access to Information Act.

Information obtained in confidence

n) information that was obtained in confidence from

i) an international organization of states or an institution thereof;

ii) the government of a province or an institution thereof;

iii) a municipal or regional government established by an Act of the legislature of a province or an institution of such a government

when the information does not relate to a class of information described in 5 b) to 5 d) above.

11. When it is determined that the compromise of specific information would be injurious to the public interest, it shall be designated as PROTECTED-1 or PROTECTED-2, according to the following criteria:

a) Government information shall be designated as PROTECTED-1 when unauthorized disclosure, destruction, removal, modification or interruption could reasonably be expected to cause serious injury to the public interest, or

b) Government information shall be designated as PROTECTED-2 when unauthorized disclosure, destruction, removal, modification or interruption could reasonably be expected to cause injury to the public interest.

12. Certain situations may arise in which a compromise of a given asset, listed in paragraph 10, would have an adverse effect upon the national interest. In that event, such an asset should be classified in the national interest and designated accordingly. Such action may be taken only after the most careful evaluation of the situation, and upon determination that no alternative course exists.

Material Assets

13. Government material assets shall be designated as PROTECTED-1 or PROTECTED-2 when unauthorized access to the material asset could reasonably be expected to cause injury to the public interest through the unauthorized disclosure of information designated as PROTECTED-1 or PROTECTED-2.

14. When unauthorized access to government material assets could reasonably be expected to cause injury to the public interest, through the destruction, removal, modification or interruption of materials or services essential to those matters to which information classified in the public interest relates, appropriate protective measures shall be considered, including where practicable, classification.

15. The specific designations shall be determined on the same basis of injury as are those for information as described in paragraph 11.

AUTHORITY TO CLASSIFY AND DESIGNATE INFORMATION AND MATERIAL ASSETS

Deputy Head makes initial determination

16. The deputy head is responsible for determining whether information and material assets of the government institution shall be classified in the national interest or in the public interest.

Deputy head has authority to designate

17. The authority to designate information and material assets as TOP SECRET, SECRET or CONFIDENTIAL in the national interest and PROTECTED-1 or PROTECTED-2 in the public interest, rests with the deputy head and will be controlled as closely as possible. On a limited basis and when operationally necessary, the deputy head may delegate this authority in writing to other officers within the government institution. These officers may appoint subordinates to exercise the delegated authority to classify on their behalf. Such delegations and appointments shall be in writing and regularly reviewed to ensure that all persons have a continuing need to exercise this authority.

Review of Designations

Responsibility to review designations

18. In conformity with the time periods specified in the directives and guidelines to be issued pursuant to this operational policy, government institutions shall review the assets which have been designated as TOP SECRET, SECRET, CONFIDENTIAL, PROTECTED-1 or PROTECTED-2 to determine if the reasons for designation have changed or are no longer valid. Whenever possible, information shall be declassified or downgraded as soon as possible.

PRINCIPLES OF PROTECTION

Principles of protection

19. In order that comprehensive and uniform protection is provided for classified assets of the government, the security programs of government institutions shall be governed by the following operational policy.

Administration of Security

Administration of security

20. The effective administration of security within the government requires that government institutions establish a security organization, incorporate security duties in position descriptions, and assign persons to be responsible for these duties.

Responsibilities of security officers

21. The deputy head of a government institution shall designate a senior official as security officer to be responsible for the development and implementation of the institution's security program. These responsibilities shall include:

a) conducting general threat assessments for the information and material assets of the government institution;

b) developing guidelines for

i) classifying and designating information and material assets,

ii) reviewing the appropriateness of assigned designations, and

iii) downgrading and declassifying information and material assets.

c) implementing security clearance procedures and advising on or implementing as required, suitability verification procedures;

d) advising on the selection and implementation of cost-effective protective measures;

e) developing and regularly reviewing protective procedures including contingency plans, and

f) conducting security education programs.

Personnel Security

22. The loyalty, reliability and suitability of individuals who are entrusted with classified assets are the base on which this security policy must rest. It is necessary therefore, to implement procedures to ensure the loyalty and associated reliability or the suitability of each such individual. These procedures will be fully described in a companion document on personnel security. For persons to be entrusted with matters classified in the national interest, the procedures must include a determination of both loyalty and associated personal reliability. For persons to be entrusted with matters classified in the public interest, the procedures will relate to a verification of suitability.

Need-to-know principle

23. In addition to these requirements, there must be a need for access to any classified assets in connection with the performance of official duties, contractual obligations or pre-contractual requirements before such access is granted. Any authorization for access to classified information shall terminate on the expiration of the purpose for which the authorization was granted.

S urity clearance requirement

24. A security clearance shall be a mandatory requirement for all persons who are to have access to assets designated as TOP SECRET, SECRET or CONFIDENTIAL.

Reliability clearance requirements

25. A verification of suitability shall be a requirement for all persons who are to have access to assets designated as PROTECTED-1 or PROTECTED-2.

Security education program

26. Through an ongoing security education program, persons who have been granted a security clearance or who occupy a position requiring a verification of suitability shall be initially advised and periodically reminded of their security duties, responsibilities and liabilities.

Sanctions

27. Any person who wilfully or negligently violates any provision of this operational policy, or the directives and guidelines issued pursuant to this operational policy, so that injury to the national or public interest occurs or could reasonably be expected to occur, may be liable to criminal or administrative sanctions.

Physical Security

Physical security of facilities and equipment

28. Physical security shall be a mandatory consideration during:

a) the planning, procurement, construction, modification or maintenance of facilities and equipment which accommodate or will accommodate classified assets, and

b) the acquisition, operation or maintenance of supporting utilities and services to the facilities and equipment.

Physical security of information and material

29. Approved methods, equipment and facilities shall be used for the physical handling, storage, transmission, transporting and disposal of classified assets.

Access control and surveillance

30. Approved methods and equipment shall be used to provide access control and surveillance to protect against unauthorized access to classified assets.

Communications - Electronic Security (COMSEC)

Cryptographic security

31. Classified information transmitted by any telecommunications system shall be protected by approved procedures, circuitry or cryptographic systems appropriate to the designation of the information involved.

Communication security

32. Equipment used in the transmission or processing of classified information shall meet approved COMSEC criteria, appropriate to the designation of the information involved.

Interconnection of systems

33. The interconnection of EDP systems and telecommunications services shall be carefully planned and coordinated to ensure that security of the

information being processed and transmitted is provided. Advice in this regard shall be requested from the appropriate authorities as indicated under paragraphs 41 a) and 41 b).

Electronic Data Processing Security

EDP security

34. Government institutions shall ensure that appropriate protection is afforded classified information processed or stored in any electronic data processing system.

Technical Intrusion Security

Technical intrusion security

35. Government institutions shall ensure that appropriate security measures are taken to protect classified information against unauthorized audio, visual, optical and electronic access.

PROTECTIVE MEASURES

Minimum standards

36. Minimum standards for the administration of this policy and the implementation of protective measures in the above six areas of security shall be described in the directives issued pursuant to this operational policy.

Protection of unclassified assets

37. Government assets which are unclassified shall be afforded custodial care in accordance with the relevant directives and guidelines in the Administrative Policy Manual issued by the Treasury Board.

Other provisions

38. The protective measures taken by government institutions shall be in accordance with and subject to any related statutory provision or Cabinet directive.

ROLES AND RESPONSIBILITIES

Responsibilities of d ity heads

39. Deputy heads, under the direction of Ministers, shall be responsible for the protection of classified assets, and for ensuring compliance with this operational policy and with the directives and guidelines to be issued pursuant to this policy.

Responsibilities of interdepartmental committees

40. Appropriate interdepartmental committees shall be responsible for:

a) providing advice to Ministers, and government institutions on the interpretation of this operational policy,

b) identifying problems related to the effectiveness of this policy and recommending appropriate changes in policy and additions or amendments to existing directives and guidelines, and

c) providing advice with respect to the resolution of security-related conflicts within the government.

ponsibil-
ities of
specific
government
agencies

41. The following government agencies shall provide security advice, assistance and auditing on a government-wide basis as indicated hereunder.

a) The Communications Security Establishment of the Department of National Defence is the national COMSEC agency and is responsible for providing guidance and advice on COMSEC matters to government institutions represented on the COMSEC community committee structure.

b) The Department of Communications is responsible for providing guidance and advice on COMSEC matters to all other government institutions, except those in 41 a) above.

c) The Department of External Affairs, except as otherwise provided, is responsible for:

i) all aspects of protective security, including the audit function, for classified information and material assets in the custody of the Department of External Affairs, including Canadian diplomatic and consular posts abroad;

ii) the inspection of the measures employed by other government institutions, except the Department of National Defence and the Canadian Forces, to protect North Atlantic Treaty Organization (NATO) documents in their custody, and

iii) conducting their own technical intrusion and physical security inspections.

d) The Department of National Defence (DND) and the Canadian Forces, except as otherwise provided, are responsible for:

i) conducting security clearance investigations for members of the Canadian Forces and persons employed by DND;

ii) all aspects of security, including the audit function, for defence establishments, assets, and operations;

iii) protecting NATO and foreign military information and material in their custody;

iv) protecting military equipment and facilities of allies which are under the control of the Minister of National Defence and the inspection of the measures employed by other government institutions to protect ATOMAL documents in their custody;

v) inspecting and evaluating their EDP facilities when their organization and operational needs, as prescribed under the authority of the National Defence Act, so dictate, and

vi) conducting their own technical intrusion security inspections.

e) The Department of Public Works (DPW) is responsible for:

i) providing physical security for government buildings while under construction by D.P.W.;

ii) providing basic physical security for the fabric of government owned buildings on the inventory of DPW; providing basic physical security for government accommodations leased by DPW; providing additional security as requested by occupying government institutions in these premises on a cost recoverable basis;

iii) providing, funding, installing and maintaining approved physical security equipment related to basic buildings constructed by D.P.W.;

iv) providing, funding and managing the basic building security guard services in multiple occupancy buildings, and

v) sharing the costs of security guard services with the tenant government institution in single occupancy buildings with commercial facilities.

f) The Department of Supply and Services (Supply Administration) is responsible for:

(i) providing advice, at the requirements definition stage, in relation to the acquisition of guard services, physical security equipment, and except as otherwise provided COMSEC and COMSEC-related items;

(ii) acquiring such goods and services, in f)i) above, and ensuring that the suppliers comply with approved standards as outlined in a contract or agreement throughout the life of that contract or agreement;

(iii) arranging for security clearances for non-government persons who are to have access to classified assets during a pre-contractual process, or under a contract or agreement, to provide goods or services through D.S.S. to the government;

(iv) ensuring the adequacy of protective measures applied at off-government premises by non-government personnel or private sector organizations which have access to or are in the custody of classified assets during a pre-contractual process, or under a contract or agreement, to provide goods or services through D.S.S. to the government, and

(v) providing advice and assistance to government institutions regarding the implementation of bilateral and multilateral industrial security agreements or arrangements.

g) Department of Supply and Services (Services Administration) is responsible for providing advice and direction to all government institutions on all aspects of the payments process under the control of the Receiver General and the Deputy Minister of Services. Such responsibilities include, payments, documents design, procuring and safekeeping; protection of payment data; payment systems and procedures; accounting practices; and other related security matters.

h) The Public Service Commission of Canada is responsible for:

i) providing direction regarding appointments made under the Public Service Employment Act to positions requiring security clearances or verification of suitability, and

ii) assisting, where required, in the provision of security training programs for employees.

i) The Royal Canadian Mounted Police (RCMP), except as otherwise provided, is responsible for:

i) assisting government institutions in determining whether to grant persons a security clearance by, where required, checking criminal and subversive records, conducting field investigations, and providing factual reports on the information revealed together with a recommendation respecting the granting or withholding of security clearances;

ii) inspecting, testing, evaluating and, where required, designing physical security equipment and developing related standards;

iii) where required, maintaining physical security equipment, uniquely designed

or modified for the protection of assets classified in the national interest;

iv) inspecting and evaluating the security aspects of government EDP facilities, as well as private sector facilities engaged in processing government information under contract and initiating related standards;

v) conducting technical intrusion security inspections;

vi) providing advice and assistance to government institutions on the implementation of the directives and guidelines to be issued pursuant to this operational policy, and when required, providing similar advice and assistance to the Treasury Board, and

vii) providing a security consulting service regarding the design of new or renovated government buildings.

Some of the above responsibilities may be removed or modified following the establishment of the Canadian Security Intelligence Service.

j) The Treasury Board, supported by the Treasury Board Secretariat, is responsible for:

i) approving, issuing and revising the directives, guidelines and standards pursuant to this operational policy, and

ii) causing the implementation and effectiveness of the directives, guidelines and standards to be monitored and audited, including the delegation of authority by Deputy Heads to designate classified assets.

k) The Ministry of the Solicitor General is responsible for assisting in the development of directives and guidelines to be issued under the authority of the Treasury Board as specified in paragraph 41 j)i).