THIS DOCUMENT HAS BEEN PREPARED BY THE SECURITY POLICY UNDER REVIEW (S.P.U.R.) SECRETARIAT FOR DISCUSSION PURPOSES ONLY

CONFIDENTIAL

November 15, 1977

DRAFT CABINET DIRECTIVE

Security in the Federal Government

SHORT TITLE

1. This directive may be cited as the Federal Security Directive.

INTERPRETATION

2. In this directive,

(a) "agency" means any corporation or entity, other than a department, that is ultimately accountable through a Minister to Parliament for the conduct of its affairs;

(b) "approved" means acceptable to the appropriate senior interdepartmental advisory committee of the Government of Canada;

(c) "asset" means any information, material or service which requires protection for reasons of national or civil security;

(d) "contingency" means any emergency, disaster or incident which could adversely affect national or civil security assets;

(e) "cryptographic system" means a system which renders plain text unintelligible and reconverts unintelligible text into intelligible language;

(f) "department" means any department named in Schedule A to the Financial Administration Act, or any other division or branch of the public service of Canada designated by the Governor in Council as a department for the purposes of that act;

(g) "deputy minister" means the deputy minister of a department;

(h) "emanation security" means measures taken to deny unauthorized access to information which might be derived from the intercept and analysis of compromising emissions from equipment used to process national or civil security information;

(i) "encryption" means the conversion of plain text into a different form in order to conceal its meaning;

(j) "fabric" means the permanent elements of a building, including the approaches, external landscaping, entrances and exits, those parts commonly used by more than one department or agency, those parts normally available to the public, and all technical areas associated with the property management function;

(k) "individual" means a Canadian citizen or a person lawfully admitted to Canada for permanent residence;

(l) "information" means signs, signals, writing, images, sound or intelligence of any nature;

(m) "keying material" means material which is changed at pre-determined intervals and which is used directly in the process of encryption and decryption;

(n) "material" means any tangible object;

(o) "national traffic" means information transmitted by a telecommunications system within Canada and intended for the exclusive use of the Government of Canada;

(p) "personnel security clearance" means the authorization by a deputy minister, head of agency, or departmental security officer for an individual to have access to, custody of, or responsibility for national or civil security assets;

(q) "protection" means the provision of administrative, personnel, physical and technical security;

(r) "restricted area" means an area accommodating national or civil security assets to which only specified individuals have authorized access;

(s) "security breach" means any incident which represents a violation of established security policy and procedures;

(t) "security designation" means the classification or categorization of information, material and services as TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED or PROTECTED;

(u) "services" means any act, assistance or work provided by a department or agency of the Government of Canada;

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

(w) "technical intrusion" means an intrusion which utilizes electromagnetic, acoustic, mechanical, photographic or other means of intercepting information, and

(x) "telecommunications" means the transmission, emission or reception of signs, signals, writing, images, sound or intelligence of any nature by wire, radio, visual or other electromagnetic system.

SECURITY REQUIREMENTS

ASSETS

3. Information, material and services owned or in the custody of the Government of Canada shall be assessed to determine if protection is required for reasons of national or civil security.

(a) Information, material and services which are sensitive with respect to the national security of Canada shall be considered (classified national security) assets. The sensitivity of (classified national security assets) shall be related to one or more of the following:

(i) international relations;
(ii) national defence;
(iii) national internal security;
(iv) national federal-provincial relations;
(v) confidences of the Queen's Privy Council for Canada, or
(vi) investigations by government institutions ~~in the areas of~~ in relation to national security, detection and suppression of crime generally or the administration or enforcement of any Act of Parliament.

(b) Information, material and services which are sensitive with respect to an individual, group, organization or government institution for reasons other than national security shall be considered (limited civil security) assets. The sensitivity of (limited civil security) assets shall be related to one or more of the following:

(i) personal privacy;
~~(ii) financial integrity;~~
(iii) commercial or proprietary considerations;
(iv) legal considerations;
(v) the decision-making process of the Government of Canada;
(vi) prohibitions established by federal enactments, or
(vii) monetary or replacement value.

THREATS

4. In order to determine appropriate protective measures, a department or agency responsible for national or civil security assets shall assess those events which can affect the confidentiality, integrity or availability of these assets. Specifically, the vulnerability of assets to the threats of accidental or deliberate disclosure, removal, modification, destruction or interruption shall be assessed.

DESIGNATIONS

5. Information, material and services shall be classified TOP SECRET only when unauthorized access could cause exceptionally grave damage to the national security.

6. Information, material and services shall be classified SECRET only when unauthorized access could cause serious damage to the national security.

7. Information, material and services shall be classified CONFIDENTIAL only when unauthorized access could be prejudicial to the national security.

8. Information, material and services shall be classified RESTRICTED only when unauthorized access could be undesirable to the national security.

9. Information, material and services shall be categorized PROTECTED only when unauthorized access could adversely affect an individual, group, organization or government institution on grounds other than national security.

10. Compilations of information or material may warrant a higher security designation than that of the component parts, because of the sensitivity created by the aggregation.

11. When feasible, national and civil security information and material shall be marked with the appropriate security designation.

12. Markings or caveats additional to TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECTED may be applied to restrict access to information and material.

13. Information or material which originates from other nations or international agencies and which bears a security designation of that nation or agency shall be afforded the same treatment as Government of Canada information or material of the equivalent security classification or categorization.

14. When possible, the duration of the security designation assigned to information or material shall be specified, as well as the circumstances under which the designation may be modified.

15. If no duration or is specified for a security designation, it shall remain in effect and the asset shall be exempted from access by the public ~~for 30 years, as prescribed in Cabinet Directive 46.~~ replace

16. A department or agency shall ~~continually~~ periodically, regularly review national and civil security assets for the purpose of modifying or eliminating security designations.

AUTHORITIES

17. The deputy minister or head of agency shall have the authority to administer and implement Government of Canada security policy and procedures. The deputy minister or head of agency shall appoint a departmental security officer to assist in carrying out departmental security responsibilities.

18. The deputy minister or head of agency shall identify those assets which require protection for reasons of national and civil security, and shall designate these assets as TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED or PROTECTED.

19. The deputy minister or head of agency may delegate the responsibility to assign security designations. All persons so delegated shall receive written instructions from the deputy minister or head of agency as to their authority and the level to which they can classify or categorize information, material and services.

unless in writing?

20. The deputy minister or head of agency shall modify the duration of the security designation of assets if he or she is satisfied that the reasons for the designation have changed or are no longer valid.

21. The security designation of information, material and services shall not be modified or eliminated without the written agreement of the originating department or agency.

SANCTIONS

22. Adherence to the policy established by this directive and the executive orders issued pursuant to it shall be the responsibility of each department and agency.

23. Sanctions related to the enforcement of this directive and the procedures issued pursuant to it are contained in the Official Secrets Act; the Financial Administration Act; the Public Service Employment Act; the Canadian Human Rights Act; the Federal Court Act; the Criminal Code; related provincial statutes, and federal statutes which create or enable the operation of departments and agencies.

FUNDAMENTAL SECURITY AREAS

24. In order to ensure that ~~complete~~ confidentiale protection is provided for national and civil security assets, the security policy and procedures of departments and agencies shall recognize four essential elements:

(a) administrative security,
(b) personnel security,
(c) physical security, and
(d) technical security. (comm, election, EDP, Courier).

ADMINISTRATIVE SECURITY

25. In order to ensure that departments and agencies achieve and maintain the essential level of administrative security:

(a) A security organization shall be established, individual security duties shall be developed, and personnel shall be assigned to be responsible for all aspects of security.
(b) Security policy and procedures shall be established and disseminated.
(c) Security threat assessments shall be conducted by:
    (i) identifying all assets which require protection for reasons of national or civil security;
    (ii) identifying the threats associated with each national or civil security asset;
    (iii) identifying the vulnerabilities of assets to these threats, and
    (iv) assessing the risk exposure associated with each asset for each threat.
(d) Based on the results of security threat assessments, appropriate safeguards shall be selected and implemented in the areas of administrative, personnel, physical and technical security.

(e) National and civil security assets shall be disseminated no further than is necessary for the discharge of Government of Canada business.

(f) Restricted areas shall be designated.

(g) Procedures shall be established to authorize, control and monitor access to national and civil security assets.

(h) Procedures shall be established for the recording, reporting and investigation of suspected security breaches.

(i) Plans to cope [deal] with all contingency situations identified by security threat assessments shall be developed and disseminated.

(j) Security procedures shall be audited and reviewed on a continuing basis.

PERSONNEL SECURITY

26. In order to ensure that departments and agencies achieve and maintain the essential level of personnel security:

(a) Positions within the department or agency where there is a requirement for access to ~~national or civil security~~ [sensitive] assets shall be ~~specified~~ [identified by security designation].

(b) Security clearance requirements for non-government personnel who work in support of government activities and who require access to ~~national or civil security~~ [sensitive] assets shall be specified.

(c) The personnel security clearance procedures issued pursuant to this directive shall be followed to determine the loyalty and reliability of personnel (government and non-government) requiring access to ~~national or civil security~~ [sensitive] assets.

(d) Personnel security clearance requirements of a more stringent nature may be applied by departments and agencies to [further] restrict access to ~~national security~~ assets [of a particularly sensitive nature].

(e) Security responsibilities shall be ~~defined~~ [outlined] in the description of duties for positions requiring access to ~~national or civil security~~ [sensitive] assets.

(f) ~~Personal identification~~ measures shall be established to ~~supervise access to and control over national and civil security~~ assets.

(g) Programs and procedures shall be implemented to ensure personnel understand, formally acknowledge, and comply with Government of Canada security policy and procedures.

PHYSICAL SECURITY

28. In order to ensure that departments and agencies achieve and maintain the essential level of physical security:

(a) Physical security shall be a mandatory consideration during the procurement, design, location, construction, installation and renovation of facilities and equipment which accommodate, or will accommodate, national and civil security assets.

(b) Physical security shall be a mandatory consideration during the provision, operation and maintenance of supporting utilities and services to facilities and equipment which accommodate national and civil security assets.

(c) Approved methods, equipment and facilities shall be utilized for the handling, storage, transportation and disposal of national and civil security information and material.

(d) Approved access control and surveillance methods and equipment shall be utilized to protect national and civil security assets.

TECHNICAL SECURITY

28. In order to ensure that departments and agencies achieve and maintain the essential level of technical security:

(a) Any department or agency planning the establishment, procurement, modification or relocation of an electronic data processing (EDP) facility, system or service shall ensure appropriate authorities are consulted in the areas of hardware, software and operations security.

(b) Control measures for data input, processing, storage and output, program generation and maintenance, and hardware operation and support shall be clearly identified in the operating procedures of the EDP facility.

(c) ~~National and civil security~~ Sensitive information transmitted by any telecommunications system over any distance shall be protected by approved cryptographic systems or by approved circuitry.

(b) EDP

(d) The interconnection of EDP systems and telecommunications services shall be carefully planned and co-ordinated to provide security for the information being processed and transmitted.

(e) Equipment used in the transmission or processing of ~~national or civil security~~ sensitive information shall meet approved emanation security criteria.

include: tested / evaluated

(f) Approved cryptographic systems shall be used for the encryption of national traffic.

(g) Approved keying material shall be used for the encryption of national traffic.

RESPONSIBILITIES

30. Each department or agency of the Government of Canada shall be responsible for ~~its own~~ security. Those under its control.

30. Institutions Security policy approved by the following bodies shall be adhered to by departments and agencies, and may be augmented by internal policy and procedures.

(a) The Cabinet Committee on Security and Intelligence (CCSI) shall consider broad policy matters in the areas of security and intelligence. ~~Recommendations~~ Issues affecting these for the approval, modification or rejection of policy shall be made to the ~~full~~ Cabinet.

omit? agencies

(b) The Interdepartmental Committee on Security and Intelligence (ICSI) shall:

(i) review Canadian security and intelligence organization activities,

(ii) provide general policy guidance to the Security Advisory Committee and the Intelligence Advisory Committee, and

(iii) provide the cabinet with the information and advice required to make decisions affecting the security of Canada.

(c) The Security Advisory Committee (SAC) shall:

(i) report to the ICSI, and the CCSI if appropriate, on the internal security situation in Canada,

(ii) formulate, for the ~~approval~~ consideration of the ICSI, general security policy and procedures for the protection of Government of Canada assets,

(iii) assist departments and agencies in the application of security policy and procedures approved by the ICSI, and

(iv) advise the ICSI on security proposals presented by a department or agency and on security matters referred by the ICSI for consideration.

(d) The Intelligence Advisory Committee (IAC) shall advise departments and agencies involved in collecting and assessing intelligence, and shall provide guidance during the formulation and implementation of policy related to national security, national defence, national sovereignty, immigration and international relations.

(e) The Interdepartmental Computer Security Panel (ICSP) shall recommend and advise on security matters relating to electronic data processing (EDP) practices, and shall review and advise on the activities of the Security Evaluation and Inspection Team (SEIT).

(f) The Communications-Electronic Security Committee (CSC) shall recommend and review policy, procedures and plans for the security of Government of Canada communications.

(g) The Security Equipment Advisory Committee shall set standards for, and approve, security equipment for Government of Canada use.

32. The following departments and agencies shall be responsible for providing advice to the Government of Canada in specific areas of security.

(a) The Privy Council Office (PCO) shall:

(i) establish liaison among departments and agencies, cabinet and inter-departmental committees on matters related to security in the Government of Canada,

(ii) co-ordinate the implementation of security directives approved by cabinet, and

(iii) participate in the formulation of security policy and procedures for recommendation to the CCSI and the ICSI.

(b) The Royal Canadian Mounted Police (RCMP) shall:

(i) advise on the implementation of physical and technical security policies of the Government of Canada;

(ii) provide advice and assistance in the completion of personnel security clearances;

(iii) organize and operate the Security Evaluation and Inspection Team (SEIT) which conducts inspections and evaluations of government EDP facilities and private sector facilities engaged in processing Government of Canada information;

(iv) conduct security surveys of Government of Canada buildings and vital points (war and peace);

(v) co-ordinate inspections to establish areas where verbal and written communications are protected from technical intrusion, and

(vi) test and rate security equipment, and install and maintain such equipment as required.

(c) The Communications Security Establishment (CSE) of the Department of National Defence shall plan, develop, evaluate and promote cost-effective communications-electronic security throughout the Government of Canada.

(d) The Department of Supply and Services (DSS) shall:

(i) ensure that suppliers of equipment and services incorporate approved security specifications,

(ii) advise regarding the acquisition of physical security equipment and guard services to be supplied by DSS,

(iii) arrange for the security clearance of non-government personnel and facilities, and

(iv) arrange for SEIT inspections of non-government EDP facilities.

(e) The Department of Communications (DOC) shall provide guidance and advice on COMSEC matters to departments and agencies not represented on the CSC.

(f) The Department of Public Works (DPW) shall ensure that suitable physical security arrangements are provided for the fabric of buildings in D.P.W. custody and, by agreement with occupying departments and agencies, may provide, operate and maintain physical security equipment and services in client accommodations.

(g) The Department of External Affairs (DEA) shall ensure appropriate security is provided for North Atlantic Treaty Organization (NATO) documents in all departments and agencies except the Department of National Defence (DND).

not for all purposes...

SECURITY PROCEDURES

32. The Interdepartmental Committee on Security and Intelligence shall approve and issue executive orders containing detailed administrative, personnel, physical and technical security procedures for the Government of Canada, consistent with the general intent of this directive.

33. The deputy minister or head of agency shall implement additional security procedures which he or she considers necessary to protect assets in his or her charge, provided they do not conflict with the policy established in this directive.