REPUBLIC OF SOUTH AFRICA

PROTECTION OF INFORMATION BILL

(As introduced by the Minister of Intelligence (National Assembly))

(The English text is the official text of the Bill)

(Minister of Intelligence)

[BXX□2008]

Bill

To provide for the protection from destruction, loss or disclosure of certain information; to provide for the regulation of the manner in which information may be protected; and to provide for matters connected therewith.

Preamble

RECOGNISING the importance of information to the security, territorial integrity and well-being of the Republic;

ACKNOWLEDGING the harm of excessive secrecy;

AFFIRMING the constitutional framework of the protection and regulation of access to information;

DESIRING to put the protection of information within a transparent and sustainable legislative framework;

AIMING to promote the free flow of information within an open and democratic society without compromising the security of the Republic.

BE IT THEREFORE ENACTED by the Parliament of the Republic of South Africa, as follows:—

CONTENTS

Section

INFORMATION WHICH REQUIRES PROTECTION AGAINST ALTERATION, DESTRUCTION OR LOSS

CHAPTER 5
INFORMATION WHICH REQUIRES PROTECTION AGAINST DISCLOSURE

Part A
Sensitive Information

Part B
Commercial and Personal Information

CHAPTER 6
CLASSIFICATION OF INFORMATION

Part A
Classification

Part B
Declassification

CHAPTER 7
DESIGNATION OF INFORMATION

CHAPTER 8
CRITERIA FOR THE CONTINUED CLASSIFICATION AND DESIGNATION OF INFORMATION

CHAPTER 9
TRANSFER OF RECORDS TO THE NATIONAL ARCHIVES

CHAPTER 10
RELEASE OF DECLASSIFIED INFORMATION TO THE PUBLIC

CHAPTER 11
IMPLEMENTATION AND MONITORING

CHAPTER 12
OFFENCES AND PENALTIES

CHAPTER 13
PROTECTION OF INFORMATION IN COURTS

CHAPTER 14
MISCELLANEOUS

CHAPTER 1
DEFINITIONS, OBJECTS AND APPLICATION OF ACT (ss 1-3)

Definitions and interpretation

1. (1) In this Act, unless the context indicates otherwise—
"**agency**" means the National Intelligence Agency referred to in section 3 of the Intelligence Services Act, 2002 (Act No. 65 of 2002);
"**archive**" means any archive established in terms of a national law or a provincial law or ordinance;
"**automatic declassification**" means the immediate declassification of certain classified information on a specified date or on the occurrence of a specified event without the need to execute any formalities or procedures;
"**categories of information**" means those groupings, types, classes, file series or integral file blocks of classified information that may be classified, designated declassified or downgraded together or in bulk;
"**categorization of information**" means the process by which state information is placed into categories for purposes of classifying or designating such information and for purposes of declassification, downgrading and the lifting of the designated status of information;
"**classification authority**" means the entity or person authorised to classify state information and includes the following persons:
(a) a head of an organ of state;
(b) officials delegated classification authority in writing by a head of organ of state;
"**classification of information**" means the process by which determinations are made as to:
(a) what levels of heightened protection to assign to certain information;
(b) who may have access to such information;
"**classified information**" is state information that has been determined under this Act or the former Minimum Information Security Standards (MISS) guidelines to be information that may be afforded heightened protection against unauthorized disclosure and has the meaning assigned to it in section 18 of this Act;
"**commercial information**" has the meaning assigned to it in section 16 of this Act;
"**confidential information**" has the meaning assigned to it in section 20(1) of this Act;
"**Constitution**" means the Constitution of the Republic of South Africa, 1996;
"**declassification authority**" means the entity or person authorised to declassify classified information and includes the following persons:
(a) the head of organ of state who authorized the original classification, if that person is still serving in the same position;
(b) the head of organ of state's current successor; or

(c) officials delegated declassification authority in writing by the head of organ of state;

"declassification database" means the database which contains all declassified information deemed by declassification authorities to be accessible by members of the public;

"declassification of information" means the authorized change in the status of information from classified information to unclassified information;

"designation authority" means the entity or person authorised to designate state information and includes the following persons:

(a) a head of an organ of state;

(b) officials delegated designation authority in writing by a head of organ of state;

"department" means a department as defined in section 1 of the Public Service Act, 1994 (Act No. 103 of 1994) and for the purposes of this Act includes organs of state;

"designated information" is information which is not in material or record form and which requires protection against unauthorised disclosure;

"downgrading of information" means—

(a) a determination that information classified and safeguarded at a specified level shall be reclassified and safeguarded at a lower level; or

(b) a determination that designated information loses its designated status;

"file series" means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, or they result from the same activity, instruction, document a specific kind of transaction; or they take a particular physical form; or they have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use;

"head of an organ of state" means—

(a) in the case of a national department, provincial administration, provincial department or organisational component mentioned in Column 1 of Schedule 1, 2 or 3 to the Public Service Act 1994 (Act No. 103 of 1994), the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of the said Schedule 1, 2 or 3 opposite the name of the relevant national department, provincial administration or organisational component or the person or the person who is acting as such;

(b) in the case of a municipality, the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998), or the person who is acting as such;

(c) in the case of any other institution, means the chief executive officer' or equivalent officer, of that public body or the person who is acting as such; or

(d) in the case of a national key point declared as such in terms of the National Key Points (Act No. 102 of 1980), the owner of the national key point;

"identifiable damage" means significant and demonstrable harm;

"information" has the meaning assigned to it in section 4 of this Act;

"information and communication technology" or **"ICT"** security means the application of security measures to protect the design, development, implementation, support, management and use of:

(a) computer-based information systems, including software applications, computer hardware and data; and
(b) electronic and mobile communication systems and the transmission of data;

"**information principles**" are those principles that guide the protection of information as set out in chapter 2 of this Act;

"**information Security**" means the safeguarding or protecting of information in whatever form and includes, but is not limited to:

(a) document security measures;
(b) physical security measures for the protection of information;
(c) information and communication technology security measures;
(d) personnel security measures;
(e) continuity planning;
(f) security screening;
(g) technical surveillance counter-measures;
(h) dealing with and reporting of information security breaches;
(i) investigations into information security breaches; and
(j) administration and organization of the security function at organs of state to ensure that information is adequately protected;

"**integral file block**" means a distinct component of a file series that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time;

"**intelligence**" means any information, obtained by any means, for the purpose of crime prevention, investigation and combating or for the purpose of informing any government decision or policy-making process carried out in order to protect national security or to further the national interest and includes the definitions of counter-intelligence, crime intelligence, departmental intelligence, domestic intelligence, domestic military intelligence, foreign intelligence and foreign military intelligence as set out in section 1 of the National Strategic Intelligence Act, 1994 (Act No. 34 of 1994);

"**intrinsic value approach**" has the meaning assigned to it in section 8 of this Act;

"**legitimate interest**" in the context of the intrinsic value approach to designating information, means an interest that is consistent with the Constitution, applicable law and the mandate of an organ, institution or department of state;

"**minister**" means the member of Cabinet designated by the President to assume the responsibility for intelligence services as contemplated in section 209 (2) of the Constitution;

"**MISS Guidelines**" means the Minimum Information Security Standards document as approved by Cabinet on 4 December 1996;

"**National Archives**" means the National Archives and Records Service of South Africa established by section 2 of the National Archives and Records Service of South Africa Act, 1996 (Act No.43 of 1996);

"**national intelligence structure**" has the meaning assigned to it in section 1 of the National Strategic Intelligence Act 34 of 1994;

"**national interest of the Republic**" has the meaning assigned to it in section 15 of this Act;

"**need-to-know**" means the need of a person with a valid security clearance to have access to such designated or classified information as may be necessary to enable him or her to perform his or her functions or duties;

"**organ of state**" means—

(a) any organ of state as defined in section 239 of the Constitution, including, but not limited to, any public entity as defined in section 1 of the Public Finance Management Act, 1999 (Act No. 1 of 1999) and section 3 of the Municipal Finance Management Act 56 of 2003;

(b) any facility or installation declared as a National Key Point in terms of the National Key Points Act, 1980 (Act No. 102 of 1980),

"**original classification authority** means the head of organ of state that the authorised the original classification, or the person or entity authorised by the head of organ of state to do so;

"**personal information**" has the meaning assigned to it in section 17 of this Act;

"**physical security**" means the use of physical measures to prevent or deter unauthorized persons from accessing protected information; and the measures deployed to detect attempted or actual unauthorized access and to activate an appropriate response;

"**protected information**" means state information which requires protection against destruction, loss or unauthorised disclosure;

"**public interest**" means all those matters that constitute the common good, well-being or general welfare and protection of the people of South Africa, the promotion of which, are required by, or are in accordance with the Constitution;

"**public record**" means a record created or received by a governmental body in pursuance of its activities;

"**record**" means recorded information regardless of form or medium;

"**regulations**" means the National Information Security Regulations and includes regulations issued by the Minister in terms of this Act;

"**secret information**" has the meaning assigned to it in section 20(2) of this Act;

"**security**" means to be protected against danger, loss or harm; and is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts;

"**security clearance**" means a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subject to the need to know;

"**security committee**" means the committee, comprising representatives from all main functions or structures of an institution, charged with overseeing the development, implementation and maintenance of the institution's security policy;

"**sensitive information**" has the meaning assigned to it in section 14 of this Act;

"**state information**" has the meaning assigned to it in section 5 of this Act;

"**state operations**" means any function, activity or process conducted by an organ of state which is authorised by law and is in accordance with the Constitution;

"**technical surveillance countermeasures**" means the process involved in the detection, localisation, identification and neutralisation of technical surveillance of an individual, an institution, facility or vehicle;

"**this Act**" includes regulations made in terms of section 59;

"**top secret information**" has the meaning assigned to it in section 20(3) of this Act.

"**unauthorised disclosure**" means the disclosure or release of protected information which is not in accordance with the policies, legislative requirements and directives of the government and the courts,
"**valuable information**" has the meaning assigned to it in section 6(2) of this Act.

(2) This Act must be interpreted to give effect to its objects and to develop the information principles set out in chapter 2.

Objects of Act

2. The objects of this Act are to—

(a) regulate the manner in which state information may be protected;
(b) promote transparency and accountability in governance while recognizing that state information may be protected from disclosure in order to safeguard the national interest of the Republic;
(c) establish general principles in terms of which state information may be handled and protected in a constitutional democracy;
(d) provide for a thorough and methodical approach to the determination of what state information may be protected;
(e) provide a regulatory framework in terms of which protected information is safeguarded in terms of this Act;
(f) define the nature and categories of information that may be protected from destruction, loss or unauthorised disclosure;
(g) provide for the classification and designation of information and the declassification of classified information and the lifting of the designated status of information;
(h) create a system for review of the status of classified and designated information by way of regular reviews and requests for review;
(i) regulate the release of declassified information to the public;
(j) harmonize the implementation of this Act with the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) and the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996);
(k) establish a National Declassification Database of declassified information that will be made accessible to members of the public;
(l) criminalize espionage and activities hostile to the Republic and provide for certain other offences and penalties; and
(m) repeal the Protection of Information Act, 1982 (Act No. 84 of 1982).

Application of Act

3. (1) This Act shall apply to—

(a) all organs of state; and
(b) juristic and natural persons to the extent that the Act imposes duties and obligations on such persons.

(2) The Minister, on good cause shown and on such terms and conditions as the Minister may determine, may by notice in the *Gazette*—

(a) exempt an organ of state or a group or class of organs of state from the application of the duty to establish departmental standards and procedures in terms of section 10 of this Act and

the duty to report to Parliament in terms of section 58 of this Act;

(b) restrict or preclude an organ or state or a group or class of organs of state from exercising the authority to classify information in terms of chapter 6 of this Act;

(c) grant to an organ of state an extension to the eighteen month period referred to in section 26 of this Act;

(d) provide an exemption to the requirement in section 26(c) of this Act that all information formerly classified as restricted be automatically declassified;

(e) exempt an organ of state from declassifying information before such information is transferred to the National Archives or other archives as required by section 38 of this Act; or

(f) exempt an organ of state from the provisions of section 42(1) which authorizes the NIA to carry out on-site inspections and reviews for the purpose of monitoring the protection of information programs.

(2) For the purpose of this Act, the Minister may, on his or her own accord or on the request of an organ of state or organs of state by notice in the *Gazette*—

(a) determine that an organ of state is to be regarded as part of another organ of state;

(b) determine that a category of organs of state is to be regarded as one organ of state with such head of organ of state as the Minister specifies; and

(c) if there is doubt as to whether an organ of state is a separate organ of state or forms part of another organ of state, determine that the organ of state—

(i) is a separate organ of state; or

(ii) forms part of another organ of state.

(3) When considering an apparent conflict between this legislation and other information-related legislation, every court must prefer any reasonable interpretation of the legislation that avoids a conflict over any alternative interpretation that results in a conflict.

CHAPTER 2
NATURE AND GENERAL PRINCIPLES OF INFORMATION (ss 4-8)

Nature of information

4. 'Information', for the purposes of this Act includes any facts, particulars or details of any kind, whether true or false, and contained in any form, whether material or not, including, but not limited to:

(a) Documents, records, data, communications and the like whether in paper, electronic, digital, audio-visual format, DVD, microform C, microfione, microfilm and microfiche form or format or any other form or format; and

(b) conversations, opinions, intellectual knowledge, voice communications and the like not contained in material or physical form or format.

State information

5. (1) State information is information generated, acquired or received by organs of state or in the possession or control of organs of state.

(2) State information is not automatically protected against disclosure.

(3) State information should be made available to the public unless there are good reasons to withhold it.

(4) State information may, in terms of this Act, be protected against disclosure, destruction, alteration or loss.

Protected information

6. (1) State information which requires protection against destruction, loss or unauthorised disclosure is referred to as "protected information".

(2) State information which requires protection against unauthorised alteration, destruction or loss is referred to as "valuable information".

(3) State information which is not in material or record form and which requires protection against unauthorised disclosure may be protected by way of designation and is thereafter referred to as "designated information".

(4) State information in material or documented form which requires protection against unauthorised disclosure may be protected by way of classification and access to such information may be restricted to certain individuals who carry a commensurate security clearance.

General Principles of State Information

7. The following principles underpin this Act and inform its implementation and interpretation:

(a) Unless restricted by law or by justifiable public or private considerations, state information should be available and accessible to all persons;

(b) information that is accessible to all is the basis of a transparent, open and democratic society;

(c) access to information is a basic human right; accessible information promotes human dignity, freedom and the achievement of equality;

(d) the free flow of information promotes openness, responsiveness, informed debate, accountability and good governance;

(e) the free flow of information can promote safety and security;

(f) accessible information builds knowledge and understanding; and promotes creativity, education, research, the exchange of ideas and economic growth;

(g) some confidentiality and secrecy is however vital to save lives, to enhance and to protect the freedom and security of persons, bring criminals to justice, protect the national security and to engage in effective government and diplomacy;

(h) measures to protect information should not infringe unduly on personal rights and liberties or make the rights and liberties of citizens unduly dependent on administrative decisions; and

(i) measures effected in terms of this Act must—
(i) have regard to the freedom of expression and the other rights and freedoms enshrined in the Bill of Rights; and
(ii) be consistent with article 19 of the International Covenant on Civil and Political Rights and have regard to South Africa's international obligations.

Intrinsic Value Approach

8. (1) The intrinsic value approach shall be used to determine what state information should be protected against unauthorised disclosure, destruction and/ or loss.

(2) The intrinsic value approach demands a reasoned and rational approach to such a determination—
(a) it should promote the effective administration of government and balance the rights of individuals with legitimate governmental requirements and objectives; and
(b) the approach involves a consideration of the content of information and the consequences of disclosure.

(3) This determination includes several considerations:
(a) Whether the organ of state in question has a legitimate interest in protecting certain information from disclosure; and
(b) A consideration of the intrinsic value of information involves:
(i) An understanding of the types and categories of information within an organ of state;
(ii) an appreciation of the inherent and essential utility and significance of the information;
(iii) an assessment of the reasonably foreseeable consequences if specific information is disclosed, altered or destroyed; and
(iv) an assessment of the protection and administrative costs associated with each type or category of information compared with the ultimate benefits of protection against disclosure, alteration or destruction.

CHAPTER 3
NATIONAL INFORMATION SECURITY STANDARDS AND DEPARTMENTAL POLICIES AND PROCEDURES (ss 9-10)

National standards and procedures

9. (1) The Minister shall, within twelve months of the commencement of this Act—
(a) prescribe broad categories of information that may be designated, classified, downgraded and declassified and protected against destruction, alteration and loss; and
(b) prescribe national information security standards and procedures for the categorisation, designation, classification, downgrading and declassification of information.

(2) The Minister may make national standards for the protection of information against destruction, alteration and loss, including but not limited to:
(a) Organization and administration of information security matters at organs of state;
(b) personnel security, including training, awareness and security screening;
(c) information and Communication Technology security;

(d) physical security for the protection of information in consultation with the Minister of Safety and Security; and

(e) continuity planning.

(3) The Minister shall publish a notice in the *Gazette* of any categories of information in terms of subsection (1)*(a)* and the Minister shall provide an opportunity for organs of state and other interested persons to submit comments.

(4) The Minister may take into account such comments before establishing categories of information in terms of subsection (1)*(a)*; and subsection (2) shall apply to any modifications to the categories of information.

(5) No measure taken under this section may impede or prevent the National Archives or any other archive from and preserving and managing public records in terms of the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996) or other applicable law or ordinance.

Departmental policies and procedures

10. (1) The head of each organ of state shall establish departmental policies, directives and categories for designating, classifying, downgrading and declassifying of the information, and the protection of information against loss and destruction, created, acquired or received by that organ of state.

(2) Departmental policies and directives shall not be inconsistent with the national information security standards made in terms of section 9.

(3) Each organ of state shall establish departmental policies, directives and categories in terms of subsection (1) within eighteen months of the commencement of this Act.

CHAPTER 4
INFORMATION WHICH REQUIRES PROTECTION AGAINST ALTERATION, DESTRUCTION OR LOSS (s11-13)

Valuable information

11. In determining if information must be regarded as valuable an organ of state must consider—

(a) if the information should be retained for later use or reference; and

(b) if the alteration, loss or destruction of such information:

(i) will impede or frustrate the State in the conduct of its functions; and

(ii) will deny the public or individuals a service or benefit to which they are entitled.

Process of determining information as valuable

12. (1) State information is determined as valuable when—

(a) information is identified in terms of a prescribed procedure or policy as information that should be protected from destruction and loss; and

(b) items of information, files, integral file blocks, file series or categories of information are entered into a departmental register of valuable information.

(2) State information is identified as valuable information through a consideration of its intrinsic value to the state and the persons and organisations that the state interacts with.

(3) Items of information, files, integral file blocks, file series or categories of state information may be determined as valuable in advance.

(4) When state information is categorized as valuable, all individual items of information that fall within a valuable category are automatically deemed to be valuable.

Protection of valuable information

13. (1) Valuable information warrants a degree of protection and administrative control and must be handled with due care and only in accordance with authorised procedures.

(2) Valuable information need not be specifically marked, but holders of such information must be made aware of the need for controls and protections as set out in the regulations.

(3) The destruction of public records is subject to the provisions of the National Archives and Records Service of South Africa Act, 1996.

CHAPTER 5
INFORMATION WHICH REQUIRES PROTECTION AGAINST DISCLOSURE

Part A
Sensitive Information (s14-15)

Nature of sensitive information

14. Sensitive information is information which must be protected from disclosure in order to prevent the national interest of the Republic from being endangered.

National interest of the Republic

15. (1) The "national interest of the Republic", for the purposes of this Act—

(a) includes all those things of benefit to the Republic and its people;

(b) is concerned with or applicable to matters important to the nation;

(c) includes all matters relating to the advancement of the public good; and

(d) includes all matters relating to the protection and preservation of all things owned or maintained for the public by the State.

(2) The national interest is multi-faceted and encompasses—

(a) the survival and security of the state and the people of South Africa; and

(b) the pursuit of justice, democracy, economic growth, free trade, a stable monetary system and sound international relations.

(3) Matters in the national interest include—

(a) security from all forms of crime;

(b) protection against attacks or incursions on South Africa or acts of foreign interference;

(c) defence and security plans and operations;
(d) details of criminal investigations and police and law enforcement methods;
(e) significant political and economic relations with international organisations and foreign governments;
(f) economic, scientific or technological matters vital to South Africa's stability, security, integrity and development.

(4) The national interest of the state must at all times be guided by the values upon which the South African state is founded, namely:
(a) Human dignity, the achievement of equality and the advancement of human rights and freedoms;
(b) non-racialism and non-sexism ;
(c) supremacy of the Constitution and the rule of law;
(d) multi-party system of democratic government, accountability, responsiveness and openness.

Part B
Commercial and Personal Information (ss 16-17)

Nature of commercial information

16. (1) Commercial information includes the commercial, business, financial or industrial information held by or in the possession of an organ of state.

(2) Commercial information becomes the subject matter of possible protection from disclosure when:
(a) Commercial information of an organ of state or which has been given by an organisation, firm or individual to an organ of state, or an official representing the state, on request or invitation or in terms of a statutory or regulatory provision, the disclosure of which would prejudice the commercial, business, financial or industrial interests of the organisation or individual concerned.
(b) when the information should be protected from disclosure in order to prevent the national interest of the Republic from being endangered.

(3) Commercial information which may prejudice the commercial, business or industrial interests of an organisation or individual, if disclosed, includes:
(a) Commercial information that is not in the public domain, which if released publicly would cause financial loss, or competitive or reputational injury to the organisation or individual concerned;
(b) trade secrets, including all confidential processes, operations, style of work, apparatus, the identity, amount or source of any income, profits, losses or expenditures of any person, firm, partnership, corporation, or association.

(4) Only commercial information which the state is not otherwise authorized by law to release may be protected against disclosure.

(5) Government-prepared reports should be protected from disclosure to the extent they restate classified commercial information.

Nature of personal information

17. Personal information is any information concerning an identifiable natural person which, if disclosed could reasonably be expected to endanger the life or physical safety of an individual.

CHAPTER 6
CLASSIFICATION OF INFORMATION (ss 18-27)

Part A
Classification (ss 18-23)

Nature of classified information

18. Classified information—

(a) is sensitive, commercial or personal information which is in material or record form;

(b) must be protected from unauthorised disclosure and when classified must be safeguarded according to the degree of harm that could result from its unauthorised disclosure;

(c) may be made accessible only to those holding an appropriate security clearance and who have a legitimate need to know to fulfill their official duties or contractual responsibilities; and

(d) is deemed to be valuable information that must be protected against destruction and loss.

Method of classifying information

19. (1) State information is classified when—

(a) a classification authority has identified information in terms of an applicable procedure or policy of this Act as information that warrants classification;

(b) the items or categories of information classified are marked or indicated with an appropriate classification; and

(c) the classified information has been entered into a departmental register of classified information.

(2) Items, files, integral file blocks, file series or categories of state information may be determined as classified. All individual items of information that fall within a classified file, integral file block, file series or category are deemed to be classified.

(3) The classification of information is determined through a consideration of its intrinsic value to the State and the persons and organisations that the State interacts with.

(4) Classification authorities shall ensure that information that is classified shall be marked with declassification instructions.

Classification levels

20. (1) State information may be classified as "Confidential" if the information is—

(a) sensitive information, the disclosure of which may be harmful to the security or interests of the state or could prejudice the Republic in its international relations;

(b) commercial information, the disclosure of which may cause financial loss to an entity or may prejudice an entity in its

relations with its clients, competitors, contractors and suppliers.

(2) State information may be classified as "Secret" if the information is—

(a) sensitive information, the disclosure of which may endanger the security or interests of the state or could jeopardize the international relations of the Republic;

(b) commercial information, the disclosure of which may cause serious financial loss to an entity; or which may endanger the security or interests of the state; or

(c) personal information, the disclosure of which may endanger the physical security of a person .

(3) State information may be classified as "Top Secret" if the information is—

(a) sensitive information, the disclosure of which may cause serious or irreparable harm to the security or interests of the state or may cause other states to sever diplomatic relations with the Republic;

(b) commercial information, the disclosure of which may have disastrous results with regard to the future existence of an entity; or cause serious and irreparable harm to the security or interests of the state; or

(c) personal information the disclosure of which may endanger the life of the individual concerned.

Authority to classify information

21. (1) Heads of organs of state are vested with the authority to classify and to reclassify information using the classification levels set out in section 20 of this Act.

(2) A head of an organ of state may delegate authority to classify to subordinate staff members.

(3) Only senior staff members may be given authority to classify information as secret or top secret.

(4) Classification decisions should be taken at a sufficiently senior level to ensure that only that information which genuinely requires protection is classified.

(5) Original classifiers must provide a written justification for each initial classification decision.

(6) Items, files, integral file blocks, file series or categories of state information may be determined as classified in advance.

(7) When state information is categorized as classified, all individual items of information that fall within a classified category are automatically deemed to be classified.

Principles of classification

22. (1) Classification decisions must be guided by the following principles:

(a) Secrecy exists to protect the national interest;

(b) classification of information may not under any circumstances be used to:

(i) conceal an unlawful act or omission, incompetence, inefficiency, or administrative error;

(ii) restrict access to information in order to limit scrutiny and thereby avoid criticism;
(iii) prevent embarrassment to a person, organization, or organ of state or agency;
(iv) unlawfully restrain or lessen competition; or
(v) prevent, delay or obstruct the release of information that does not require protection under this Act;

(c) the classification of information is an exceptional measure and should be used sparingly;

(d) information should only be classified when there is a clear and justifiable need to do so. A clear and justifiable need to classify information exists when there is a demonstrable need to protect the information in the national interests;

(e) if there is significant doubt as to whether information requires protection, it should not be classified;

(f) the decision to classify information must be based solely on the guidelines and criteria set out in this Act, the regulations and policies made in terms of this statutory framework;

(g) state information that does not meet the criteria set out in this Act, the regulations and applicable policies may not be classified;

(h) the decision to classify shall not be based on any extraneous or irrelevant reason;

(i) classification decisions ought to assess and weigh the benefits of secrecy with factors such as the:
(i) vulnerability of the information;
(ii) threat of damage from its disclosure;
(iii) risk of loss of the information;
(iv) value of the information to adversaries;
(v) cost of protecting the information; and
(vi) public benefit to be derived from the release of the information;

(j) scientific and research information not clearly related to the national security and the national interest may not be classified;

(k) information may not be reclassified after it has been declassified and released to the public under proper authority;

(l) when classification is resorted to, it should be in place only for as long as the protection is actually necessary; and

(m) where there is still a need for classification it may be that the information in question no longer requires high level classification and should be downgraded to a lower level of classification.

(2) The application of the classification principles shall not in any way impede or prevent law enforcement or intelligence functions and/or duties authorised or prescribed by law.

Report and Return of Classified Records

23. A person who is in possession of a classified record knowing that such record has been communicated, delivered or made available outside of the manner and purposes of this Act, except where such possession is for any purpose and in any manner authorized by law,

shall report such possession and return such record to a member of the South African Police Service or the National Intelligence Agency.

Part B
Declassification (ss 24-27)

Authority to declassify information

24. (1) The organ of state that classified information shall be responsible for its declassification and downgrading.

(2) The head of the organ of state is the declassification authority, but he or she may delegate declassification and downgrading authorities in writing to specified officials within the organ of state.

(3) The head of organ of state retains accountability for any decisions taken by such delegated authority.

(4) The National Intelligence Agency (NIA) shall be responsible for the handling of classified records and the declassification of such records of a defunct organ of state or agency that has no successor in function.

(5) The NIA shall consult with organs of state or agencies having primary subject matter interest before making final declassification determinations.

(6) Items, files, integral file blocks, file series or categories of state information may be determined as declassified. All individual items of information that fall within such a declassified category are deemed to be declassified.

Automatic declassification

25. (1) Automatic declassification is the immediate and self-executing declassification of information based upon the:

(a) Occurrence of a specific date or event, as determined by the original classification authority; upon the occurrence of which, the information will no longer need protection;

(b) expiration of a maximum time frame for duration of classification as determined by the original classification authority, which must be less than the initial protection period; or

(c) expiration of a maximum time frame for classification in terms of this Act.

(2) Classified information may not be protected for longer than the protected periods referred to in section 27.

Automatic declassification of all classified information

26. At the expiry of the period referred to in section 62(1) of this Act all classified information, which:

(a) Was classified on or before 10 May 1994 shall be automatically declassified, unless such information is classified in terms of this Act;

(b) is more than 20 years old from the date of original classification shall be automatically declassified, unless such information is classified in terms of this Act; or

(c) was formerly classified as "restricted" shall be automatically declassified, except as provided for in section 3(2)*(d)* of this Act .

Maximum protection periods

27. (1) Information may not remain classified for more than a 20-year period unless the head of the organ of state that classified the information, certifies to the satisfaction of his or her Minister, having regard to the criteria contained in chapter 8 of this Act, that continued protection of the information from unauthorized disclosure is:

(a) critical to the national security of South Africa;

(b) necessary to prevent identifiable damage to the national interest; or

(c) necessary to prevent demonstrable physical or life threatening harm to a person or persons.

(2) No information may remain classified or protected from disclosure more than 30 years from the date of its original classification unless the head of organ of state certifies to the satisfaction of his or her Minister that demonstrable life threatening or physical harm to a person or persons will result from its release.

CHAPTER 7
DESIGNATION OF INFORMATION (ss 28-32)

Nature of designated information

28. State information, which is sensitive, commercial or personal information and which is not in material or record form, may be designated as protected from unauthorised disclosure when such information, if it was recorded in material form, would have been classified in terms of Chapter 6 of this Act.

Method of designating information

29. (1) State information or categories of state information are designated when the information emerging from identified deliberations, exchanges or communications is determined in terms of an applicable procedure or policy by a designation authority as information that should be protected from unauthorised disclosure: Provided that—

(a) the state information in question is identified as designated information through a consideration of its intrinsic value to the state and the persons and organisations that the state interacts with; or

(b) State information or categories of state information emerging from or considered in identified deliberations and communications are designated in advance.

(2) All individual items of information that fall within an identified category of state information are automatically deemed to be designated.

Protection of designation information

30. (1) Holders of designated information must be made aware of the need for controls as set out in the regulations.

(2) Designated information may only be communicated to persons who have a legitimate need to know to fulfill their official duties or contractual responsibilities.

(3) Designated information is only to be released in accordance with the policies of organs of state, legislative requirements, directives of government and the orders of courts.

Authority to lift the designated status of information

31. (1) The organ of state that designated information shall be responsible for the lifting of the designated status of the information.

(2) The head of the organ of state shall have the authority to lift the designated status of information, but he or she may delegate such authority in writing to specified officials within the organ of state.

(3) The head of organ of state retains accountability for any decisions taken by such delegated authority.

(4) The National Intelligence Agency (NIA) shall be responsible for the lifting of the designated status of information of a defunct organ of state or agency that has no successor in function.

Automatic lifting of the designated status of information

32. (1) Automatic lifting of the designated status of information is the immediate and self-executing lifting of such status based upon the:

(a) Occurrence of a specific date or event, as determined by the original designation authority; upon the occurrence of which, the information will no longer need protection; or

(b) expiration of a maximum time frame for duration of designation as determined by the original designation authority.

(2) All designated information which is 10 years old from the date of its original designation, shall without any exceptions, automatically lose its designated status.

CHAPTER 8
CRITERIA FOR THE CONTINUED CLASSIFICATION OR DESIGNATION OF INFORMATION (ss 33-37)

Considerations for the continued classification or designation of information

33. (1) In taking a decision whether or not to continue the classification or designation of information, a head of an organ of state shall consider whether the lifting of the designated status of information or the declassification of classified information is likely to cause significant and demonstrable harm to the national interest of the Republic.

(2) Specific considerations may include whether the disclosure may:

(a) Expose the identity of a confidential source, or reveal information about the application of an intelligence or law enforcement method, or reveal the identity of an intelligence or

police source when the unauthorized disclosure of that source would clearly and demonstrably damage the national interests of the Republic;

(b) clearly and demonstrably impair the ability of government to protect officials or persons for whom protection services, in the interest of national security, are authorized;

(c) seriously and substantially impair national security, defence or intelligence systems, plans or activities;

(d) seriously and demonstrably impair relations between South Africa and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of South Africa;

(e) violate a statute, treaty, or international agreement, including an agreement between the South African government and another government;

(f) cause financial loss to a non-state institution or will cause substantial prejudice to such an institution in its relations with its clients, competitors, contractors and suppliers; or

(g) cause life threatening or other physical harm to a person or persons.

Regular reviews of classified and designated information

34. (1) At least once every 10 years, a head of organ of state shall review the classified and designated status of all classified and designated information held or possessed in his or her organ of state.

(2) The first 10 year period referred to in subsection (1) shall commence on the effective date of this Act.

(3) The status of classified or designated information must be reviewed when there is any need or proposal to use that information in a public forum such as in a court or tribunal proceedings.

(4) The criteria for the continued classification and designation of information as set out in this chapter shall be of application in reviews carried out in terms of this section.

(5) Organs of state shall inform the Minister and the public of the results of the regular reviews.

Requests for status reviews of classified and designated information

35. (1) Requests for the declassification of classified information or the lifting of the designated status of information may be submitted to a head of an organ of state by interested non-governmental parties and individuals.

(2) Such requests must be in furtherance of a genuine research interest or a legitimate public interest.

(3) In conducting such a review a head of an organ of state shall take into account the considerations for the continued classification or designation of information as set out this chapter.

(4) Heads of organs of state shall, in the departmental standards and procedures—

(a) develop procedures to process requests for the review of the classified or designated status of specified information; and

(b) provide for the notification to the requester of the right to appeal a decision as provided for in section 37.

(5) The procedures referred to in subsection (4) shall be implemented within eighteen months of the commencement date of the Act.

(6) In response to a request for the review of the classified status of information in terms of this Act an organ of state may refuse to confirm or deny the existence or nonexistence of information whenever the fact of its existence or nonexistence is itself classified.

Status review procedure

36. (1) Requests for a review of the classified or designated status of information shall describe the document or materials containing the information or category or categories of information with sufficient specificity to enable the organ of state to locate it with a reasonable amount of effort.

(2) An organ of state receiving a request for a review of the status of classified or designated information shall make a determination within 90 calendar days of the date of receipt of such request.

Appeal procedure

37. (1) If the head of an organ of state denies a request for declassification or the lifting of the designated status of information to a member of the public or a non-governmental organisation or entity, such person or body may appeal such decision to the Minister of the organ of state in question.

(2) All appeals to the Minister of the organ of state in question shall be lodged within 30 calendar days of receipt of the decision and reasons of the refusal from the head of the organ of state.

(3) A Minister of an organ of state who receives an appeal in terms of this section shall make a finding within 90 calendar days of the date of receipt of such request.

CHAPTER 9
TRANSFER OF RECORDS TO THE NATIONAL ARCHIVES (s 38)

Transfer of Public Records to the National Archives

38. (1) Organs of state shall review the classification of information before it is transferred to the National Archives or other archives established by law.

(2) Public records, including records marked classified that are transferred to the National Archives or other archives shall be deemed to be automatically declassified.

(3) Organs of state that hold classified records that originated in another organ of sate are required to notify the originating organ of state before transferring classified records to the National Archives or other archives and must abide by the reasonable directions of the originating organ of state.

(4) Classified records held by the National Archives or other archives at the commencement of this Act, which have been classified for less than 20 years, shall be subject to the provisions of this Act.

(5) An organ of state, which transferred classified information to the National Archives or other archives before the commencement of this Act, retains its responsibilities in terms of this Act.

(6) Where an organ of state fails to act in terms of part B of chapter 6 of this Act, classified records in possession of the National Archives or other archives shall be deemed to be automatically declassified at the expiry of the relevant protection periods referred to in sections 26 and 27 of this Act.

(7) There is no onus or obligation on the part of the National Archives or other archives to advise or notify organs of state of their responsibilities and obligations with regard to classified information in the possession of the National Archives or other archives.

CHAPTER 10
RELEASE OF DECLASSIFIED INFORMATION TO THE PUBLIC (ss 39-41)

Release of declassified information or formerly designated information to the public

39. (1) Classified information that is declassified or information that has had its designated status lifted may be released to the public in accordance with national and departmental policies and procedures, legislative requirements, inclusive of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), and orders of courts.

(2) Unless ordered by a court, no classified information may be released to the public until such information has been declassified.

(3) When an organ of state receives a request for records in its possession that contain information that was originally classified or designated by another organ of state, it shall refer the request and the pertinent records to the originating organ of state for processing, and may, after consultation with the originating body, inform any requester of the referral.

(4) There is no automatic disclosure of declassified information to the public unless that information has been placed into the National Declassification Database as provided for in section 41 of this Act.

Request for classified information in terms of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)

40. (1) A request for access to a record, as defined in the Promotion of Access to information Act, whether classified or declassified in terms of this Act, must be made in terms of the Promotion of Access to Information Act, 2000.

(2) A head of organ of state considering a request for a record which contains classified information must consider the classification and may declassify such information.

(3) If a head of organ of state decides to grant access to the requested record then he or she must declassify the classified information before releasing the information.

(4) Should a refusal to grant access to such a classified record be taken on appeal in terms of the Promotion of Access to Information Act, the relevant appeal authority must consider the classification and may declassify such information.

Establishment of a National Declassification Database

41. (1) The National Archives and Records Services of South Africa shall, in conjunction with those organs of state that originate classified information, establish a government wide database of declassified information that heads of organs of state have determined may be made available to the public: Provided that no declassified information may be placed in the National Declassification Database, if access to such information may be refused in terms of the Promotion of Access to Information Act.

(2) This database shall be known as the National Declassification Database and shall be located at the National Archives and Records Services of South Africa.

(3) The National Archives and Records Services of South Africa shall be responsible for the management and maintenance of the National Declassification Database.

(4) Heads of organs of state shall cooperate fully with the National Archives of South Africa in the establishment and ongoing operations of the Database.

(5) The Department of Defence Archive Repository as provided for in section 83(3) of the Defence Act, 2002 (Act No. 42 of 2002) shall be part of the National Declassification Database.

(6) Information contained within the Database shall, at a reasonable cost, be made available and accessible to members of the public.

CHAPTER 11
IMPLEMENTATION AND MONITORING
(ss 42-43)

Responsibilities of the National Intelligence Agency

42. (1) The National Intelligence Agency (NIA) shall be responsible for:

(a) monitoring of the national protection information policies and programmes carried out by organs of state ;

(b) on-site inspections and reviews for the purpose of monitoring the protection of information programs;

(c) provision of expert support and advice:

(i) to organs of state which require assistance in the handling of requests for the review of the status of classified and designated information;

(ii) to Ministers who require assistance in the determination of appeals in terms of section 37 of this Act;

(d) making of recommendations to heads of organs of state and the Minister based on its findings;

(2) The NIA shall provide the following guidance and support to organs of state:

(a) development, coordination, support and facilitation of the implementation of national policies in an efficient, cost-effective and consistent manner across all organs of state;

(b) promotion of partnerships with organs of state and the enhancement of cooperation between different departments;

(c) provision of expert support and advice:

(i) to organs of state which require assistance in the classification and declassification of information;

(ii) to organs of state which require assistance in the designation of information and the lifting of the designated status of information; and

(iii) to organs of state which require assistance in the carrying out of regular reviews of classified and designated information;

(d) identification and exploration of best departmental practices;

(e) development of education materials and running of training and awareness programmes;

(f) creation of pilot projects to develop new methodologies to facilitate streamlined programmes;

(g) exploration of uses of technology to facilitate the declassification process; and

(3) Subsections (1) and (2) shall not apply to the South African Police Service and the South African National Defence Force.

Dispute Resolution

43. If disputes arise between the NIA and any organ of state or agency in relation to any of the responsibilities of NIA referred to in section 42, the head of the organ of state concerned or the NIA may refer the matter to the Minister for resolution of the dispute.

.

CHAPTER 12
OFFENCES AND PENALTIES (ss 44-56)

Espionage Offences

44. (1) It is an offence punishable by imprisonment for a period not exceeding twenty-five years:

(a) To communicate, deliver or make available state information with the intention to give advantage to another state; or

(b) to make, obtain, collect, capture, or copy a record containing state information with the intention to give advantage to another state,

where, if the information is sensitive information, the disclosure of which may cause serious or irreparable harm to the security or interests of the state or may cause other states to sever diplomatic relations with the Republic; if the information is commercial information, the disclosure of which may cause serious or irreparable harm to the security or interests of the state; or if the information

is personal information the disclosure of which may endanger the life of an individual.

(2) It is an offence punishable by imprisonment for a period not exceeding fifteen years:

(a) To communicate, deliver or make available state information with the intention to give advantage to another state; or

(b) to make, obtain, collect, capture or copy a record containing state information with the intention to give advantage to another state,

where, if the information is sensitive information, the disclosure of which may endanger the security or interests of the state or could jeopardize the international relations of the Republic; if the information is commercial information, the disclosure of which may endanger the security or interests of the state; or, if the information is personal information, the disclosure of which may endanger the physical security of an individual.

(3) It is an offence punishable by imprisonment for a period not exceeding five years:

(a) To communicate, deliver or make available state information with the intention to give advantage to another state; or

(b) to make, obtain, collect, capture or copy a record containing state information with the intention to give advantage to another state,

where, if the information is sensitive information, the disclosure of which may be harmful to the security or interests of the state or could prejudice the Republic in its international relations.

Hostile Activity Offences

45. (1) It is an offence punishable by imprisonment for a period not exceeding twenty-five years:

(a) To communicate, deliver or make available state information with the intention to prejudice the state; or

(b) to make, obtain, collect, capture or copy a record containing state information with the intention to prejudice the state,

where, if the information is sensitive information, the disclosure of which may cause serious or irreparable harm to the security or interests of the state or may cause other states to sever diplomatic relations with the Republic; if the information is commercial information, the disclosure of which may cause serious or irreparable harm to the security or interests of the state; or if the information is personal information the disclosure of which may endanger the life of the individual concerned.

(2) It is an offence punishable by imprisonment for a period not exceeding fifteen years:

(a) To communicate, deliver or make available state information with the intention to prejudice the state; or

(b) to make, obtain, collect, capture or copy a record containing state information with the intention to prejudice the state,

where, if the information is sensitive information, the disclosure of which may endanger the security or interests of the state or could jeopardize the international relations of the Republic; if the information is commercial information, the disclosure of which may endanger the security or interests of the state; or, if the information is personal information, the disclosure of which may endanger the physical security of an individual.

(3) It is an offence punishable by imprisonment for a period not exceeding five years:

(a) To communicate, deliver or make available state information with the intention to prejudice the state; or

(b) to make, obtain, collect, capture or copy a record containing state information with the intention to prejudice the state,

where, if the information is sensitive information, the disclosure of which may be harmful to the security or interests of the state or could prejudice the Republic in its international relations.

Harbouring or concealing persons

46. Any person who harbours or conceals any person whom he or she knows, or has reasonable grounds to believe or suspect, has committed, or is about to commit, an offence under sections 44 and 45, is guilty of an offence and liable to imprisonment for a period not exceeding ten years.

Interception of or interference with classified information

47. (1) Subject to the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002), a person who intentionally accesses or intercepts any classified information without authority or permission to do so, is guilty of an offence and liable to imprisonment for a period not exceeding ten years.

(2) A person who intentionally and without authority to do so, interferes with classified information in a way which causes such information to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence and liable to imprisonment for a period not exceeding ten years.

(3) A person who produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed to overcome security measures for the protection of state information, for the purpose of contravening this section, is guilty of an offence and liable to imprisonment for a period not exceeding ten years.

(4) A person who utilizes any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect state information, is guilty of an offence and liable to imprisonment for a period not exceeding ten years.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence and liable to imprisonment for a period not exceeding ten years.

Registration of Intelligence Agents and Related Offences

48. (1) Any person within the Republic or residing within the Republic and who is—

(a) employed or operating as intelligence or security agents for a foreign intelligence or security service; or

(b) who is not employed or operating as intelligence or security agents for a foreign intelligence or security service but is in the Republic with the expectation or potential of activation or re-activation as an agent of such an intelligence or security service must register with the National Intelligence Agency.

(2) Any person who fails to register as an intelligence or security agent in accordance with the provisions of this section is guilty of an offence and liable to imprisonment for a period not exceeding five years.

Attempt, conspiracy, and inducing another person to commit an offence

49. Any person who attempts; conspires with any other person; or aids, abets, induces, instigates, instructs or commands, counsels or procures another person to commit an offence in terms of this Act, shall be guilty of an offence and liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.

Disclosure of Designated or Classified Information

50. Any person who discloses designated or classified information outside of the manner and purposes of this Act except where such disclosure is for any purpose and in any manner authorized by law is guilty of an offence and liable to imprisonment for a period not exceeding five years.

Knowing Possession of Classified Information

51. Any person who fails to comply with section 23 of this Act is guilty of an offence and liable to a fine or imprisonment for a period not exceeding five years or to both such fine and imprisonment.

Provision of false information to a national intelligence structure

52. Any person who provides information to a national intelligence structure with the knowledge that such information is false or has been fabricated shall be guilty of an offence and liable to imprisonment for a period not exceeding five years.

Destruction or Alteration of Valuable Information

53. Any person who destroys or alters valuable information, except where such destruction or alteration is for any purpose and in any manner authorized by law, is guilty of an offence and liable to a fine or imprisonment for a period not exceeding three years.

Improper Classification or Designation

54. Any person who knowingly classifies or designates information in order to achieve any purpose ulterior to this Act, including the classification or designation of information in order to

conceal breaches of the law and/ or to promote or further an unlawful act; inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; or to give undue advantage to anyone within a competitive bidding process is guilty of an offence and liable to a fine or imprisonment for a period not exceeding three years.

Extra-territorial application of Act

55. Any act constituting an offence under this Act and which is committed outside the Republic by any South African citizen or any person domiciled in the Republic shall be deemed to have been committed also in the Republic.

Authority of National Director of Public Prosecutions required for institution of criminal proceedings

56. No trial or preparatory examination in respect of any offence under this Act which carries a penalty of imprisonment of five years or more shall be instituted without the written authority of the National Director of Public Prosecutions.

CHAPTER 13
PROTECTION OF INFORMATION IN COURTS (s 57)

Protection of state information before courts

57. (1) Classified information that is placed before a court may not be disclosed to persons not authorised to receive such information unless a court, in the interests of justice, orders full or limited disclosure, with or without conditions.

(2) Until a court orders the disclosure of classified information or orders the limited or conditional disclosure of classified information, the court shall issue directions for the proper protection of such information during the course of legal proceedings, which may include—

(a) the holding of proceedings, or part thereof, *in camera*;

(b) the protection from disclosure and publication of those portions of the record containing the classified information; or

(c) the implementation of measures to confine disclosure to those specifically authorised to receive the information.

(3) A court may not order the disclosure of classified information without taking reasonable steps to obtain the written or oral submissions of the classification authority that made the classifications in question, alternatively the submissions of the Director-General of the National Intelligence Agency or his or her representative.

(4) The submissions referred to in subsection (3) may not be publicly disclosed and any hearing held in relation to the determination referred to in subparagraph (1) must be held *in camera* and persons not authorised to receive such information may not attend such hearings unless authorised by a court.

(5) A court may, if it deems appropriate, seek the written or oral submissions of interested parties, persons and organisations but may not disclose the actual classified information

to such persons or parties prior to its order to disclose the information in terms of subsection (1).

(6) A classification authority, alternatively the Director-General of the National Intelligence Agency, shall declassify information required in legal proceedings, either in whole or in part, unless it is strictly necessary to maintain the classification in terms of the provisions of this Act.

(7) In addition to the measures set out in this section, a court in criminal proceedings shall have the same powers as those conferred upon a court by section 154 (1) of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), and the provisions of subsections (1) and (4) of the said section 154 shall apply mutatis mutandis,

(8) Any person who discloses or publishes any classified information in contravention of an order or direction issued by a court in terms of this section shall be shall be liable to be prosecuted in terms of section 52 of this Act.

(9) The head of an organ of state may apply to a court for an order restricting the disclosure of unclassified state information that is part of, or is intended to be part of an open court record, which if more publicly disclosed or published may undermine the national interest. A court hearing such an application may—

(a) determine its own procedures and may impose limitations on the disclosure of the information in question pending its decision to restrict disclose or not; and

(b) if it deems appropriate, invite written or oral submissions from other interested parties.

(8) A court acting in terms of this section shall endeavour to accommodate the principle of open justice to as great an extent as possible without risking or compromising the national interest.

CHAPTER 14
MISCELLANEOUS (ss 58-62)

Reports

58. (1) Each head of an organ of state shall, by no later than 31 December of each year, submit a report to his or her Minister that describes the application of the protection of information policies and procedures, and in particular the application of the classification and declassification standards and procedures of that organ of state during the preceding year. At the same time that heads of organs of state submit their reports to their respective Ministers, copies of such reports must be forwarded to the Minister, and the NIA.

(2) The NIA shall by no later than 31 December of each year, submit an annual report to the Minister on the execution of its responsibilities in terms of this Act.

(3) The NIA, shall report annually to Parliament on monitoring carried out in terms of this Act and on the status of protection of information practices by all government bodies.

(4) At the same time that the NIA, is submitted to Parliament, copies of the annual report shall be forwarded to heads of organs of state.

Regulations

59. (1) The Minister must make regulations consistent with this Act in order to provide for, *inter alia*:

(a) the controls and measures required to effectively protect valuable, designated and classified information, including the appropriate physical security, information and communication technology security, technical surveillance countermeasures and contingency planning for the protection of information;

(b) the responsibilities of heads of an organ of state to ensure that valuable, designated and classified information are adequately protected;

(c) training and guidance to be supplied to state employees on responsibilities to ensure that valuable, designated and classified information are adequately protected;

(d) the organization and administration of the security function at organs of state to ensure that information is adequately protected, including the establishment of security committees and security policies within organs of state;

(e) the efficient and effective operation of a personnel security clearance system;

(f) a procedure for the classification and protection of commercial information not in hands of the state;

(g) the marking of classified documents;

(h) restrictions on how classified information may be transferred from one person to another and from one institution to another;

(i) measures to prevent the over-classification or designation of information, including training and guidance to be supplied to staff members on how to classify and designate information and how to prevent the over-classification and designation of information;

(j) the roles of the National Intelligence Structures as defined in the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), with regard to the protection of information;

(k) the reporting of security breaches at organs of state; and

(l) the procedure to be followed for the issue of and the specific topics to be covered by the National Information Security Standards to be made in terms of section 9(1)*(b)* and *(c)* of this Act.

(2) The Minister must make the regulations referred to in subsection (1) within eighteen months of the commencement of this Act.

Transitional provisions

60. (1) The provisions of this Act are suspended from operation pending the establishment of the standards, policies and procedures referred to in chapter 4 and the regulations referred to in section 59 of this Act, or for a period of 18 months from the commencement of this Act, whichever occurs first, with the exception of—

(a) chapter 4;

(b) section 23, which provides for the reporting and return of classified records;

(c) section 39, which provides for the release of declassified information or formerly designated information to the public;

(d) section 40, which provides for requests for access to classified information in terms of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
(e) section 41, which provides for the establishment of the National Declassification Database;
(f) Chapter 11, which sets out the responsibilities of the NIA;
(g) section 59, which provides for the making of regulations; and
(h) the definitions and principles which give effect to the sections referred to in paragraphs *(a)* to *(g)*.

(2) During the period referred to in subsection (1) the following provisions of this Act shall be applied to the implementation and interpretation of the Minimum Information Security Standards—
(a) the General Principles of State Information set out in section 7;
(b) the Intrinsic Value Approach to determine what information should be protected against disclosure or destruction as set out in chapter 3;
(c) the Principles of Classification set out in section 22.

(3) During the period referred to in subsection (1) the following offences, penalties and provisions provided for in chapter 12 of this Act shall be of force and effect—
(a) section 44 which provides for espionage offences;
(b) section 45 which provides for hostile activity offences;
(c) section 46 which provides for the offence of harbouring or concealing of persons;
(d) section 47 which provides for the offence of unauthorised access to, interception of or interference with classified information;
(e) section 48 which provides for the registration of intelligence agents and related offences;
(f) section 49 which provides for the offences of attempt, conspiracy and inducing another person to commit an offence if such offence is listed in subsection (3) of this section;
(g) section 50 which provides for the offence of disclosure of designated or classified Information shall apply only in respect of classified information;
(h) section 51 which provides for the offence of knowing possession of classified information, but shall not include classified information that carries a "restricted" classification in terms of the Minimum Information Security Standards;
(i) section 52 which provides for the offence of the knowing provision of false information to a national intelligence structure;
(j) section 53 which provides for the offence of the destruction of valuable information shall apply only in respect of classified information that carries a "Restricted", "Confidential", "Secret" or "Top Secret" classification in terms of the Minimum Information Security Standards;
(k) section 54 which provides for the offence of improper classification shall apply only in respect of classified information that carries a "Confidential", "Secret" or "Top Secret" classification in terms of the Minimum Information Security Standards;
(l) section 55 which provides for the extra-territorial application of the Act in certain circumstances;

(m) section 56 which provides for the requirement of the authority of the National Director of Public Prosecutions to institute certain criminal proceedings; and

(n) Chapter 13 which provides for a procedure for the use of classified information in legal proceedings.

Repeal of laws

61. (1) The Protection of Information Act 84 of 1982 shall be repealed.

(2) Section 83(3)*(c)* of the Defence Act, 2002 (Act No. 42 of 2002), shall be repealed at the end of the period referred to in section 62(1).

Short title and commencement

62. This Act shall be called the Protection of Information Act, 2008, and shall come into operation on a date fixed by the President by proclamation in the *Gazette*.