Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID-AFRIKA

Vol. 537 Pretoria, 5 March Maart 2010 No. 32999

CONTENTS · INHOUD

GENERAL NOTICE

NOTICE 197 OF 2010

State Security Agency

EXPLANATORY SUMMARY ON THE PROTECTION OF INFORMATION BILL, 2009

The Minister of State Security intends to introduce the Protection of information Bill, 2009 in the National Assembly. The explanatory summary of the Bill is hereby published in accordance with Rule 241(c) of the National Assembly.

The Bill has been drafted to achieve the following, amongst others:

(a) create a statutory framework for the protection of State information. State information is information generated by organs of State or is in the possession or control of organs of State;

(b) set out criteria and processes in terms of which State information may be protected from destruction or from unlawful disclosure;

(c) set out criteria and processes in terms of which information which is protected from disclosure and which is classified, may be declassified;

(d) create offences and proposed sentences for unlawful disclosure of information, including the crime of espionage;

(e) make it an offence for an individual to knowingly supply false information to the national intelligence structures;

(f) establish guidelines for the treatment by courts of classified documents;

(g) provide for the Minister of State Security to issue regulations on information security across government; and

(h) repeal the existing Protection of Information Act (Act No. 84 of 1982).

Copies of the Bill as certified by the State Law Advisor can be obtained from:

The Public Liaison Officer (State Security)
Thabile Mhlamvu
Bogare Building
Corner Atterbury Road and Lois Avenue
MENLYN
0077

Tel: (012) 367 0791
E-mail: tmhlamvu@intelligence.gov.za

REPUBLIC OF SOUTH AFRICA

PROTECTION OF INFORMATION BILL

[As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. 32999 of 5 March 2010]
(The English text is the official text of the Bill)

(MINISTER OF STATE SECURITY)

[B —2010]

ISBN 978-1-77037-???-?

No of copies printed 1 800

BILL

To provide for the protection of certain information from destruction, loss or unlawful disclosure; to regulate the manner in which information may be protected; to repeal the Protection of Information Act, 1982; and to provide for matters connected therewith.

PREAMBLE

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

ACKNOWLEDGING the harm of excessive secrecy;

AFFIRMING the constitutional framework for 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

CHAPTER 1

DEFINITIONS, OBJECTS AND APPLICATION OF ACT

Definitions and interpretation

1. (1) In this Act, unless the context indicates otherwise—

"Agency" means the State Security Agency established in terms of Proclamation No. 59 of 2009 as published in Government *Gazette* No. 32566 of 11 September 2009, and includes the National Intelligence Agency, the South African Secret Service, Electronic Communications Security (Pty) Ltd (COMSEC), and the South African National Academy for Intelligence;

"archive" means any archive established in terms of a national or a provincial law;

"categories of information" means those groupings, types, classes, file series or integral file blocks of classified information that may be classified, declassified or downgraded together or in bulk;

"categorisation of information" means the process by which state information is placed into categories for purposes of classifying such information and for purposes of declassification and downgrading of information;

"classification authority" means the entity or person authorised to classify State information, and includes—

(a) a head of an organ of state; or

(b) any official to whom the authority to classify State information has been delegated in writing by a head of an organ of state;

"classification of information" means a process used to determine—

(a) the level of protection assigned to certain information; and

(b) the manner in which such information may be accessed and classified in terms of section 15;

"classified information" means the state information that has been determined under this Act or the former Minimum Information Security Standards guidelines to be information that may be afforded heightened protection against unlawful disclosure;

"commercial information" means commercial, business, financial or industrial information held by or in the possession of an organ of state;

"confidential information" has the meaning assigned to it in section 15(1);

"Constitution" means the Constitution of the Republic of South Africa, 1996;

"declassification authority" means the entity or person authorised under section 19 to declassify classified information;

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

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

"department" means a department as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994);

"downgrading of information" means a change of classified and safeguarded information from its status to be reclassified and safeguarded at a lower level;

"file series" means file units or documents that are arranged according to a filing system or kept together because they—

(a) relate to a particular subject or function;

(b) result from the same activity, instruction, document or a specific kind of transaction;

(c) take a particular physical form; or

(d) have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use;

"foreign State" means any State other than the Republic of South Africa;

"head of an organ of state" means—

(a) in the case of a department, the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994 (Proclamation No 103 of 1994), 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, 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" means 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, microphone, 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;

"information and communication technology 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" means the principles that guide the protection of information as set out in Chapter 2;

"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 organisation 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 must be maintained as a separate unit to ensure the integrity of the records, and may include a set of records covering either a specific topic or a period of time;

"intelligence" means any information, obtained by a national intelligence structure, 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 following:

(a) "Counter-intelligence", which means measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations, to protect intelligence and any classified information, to conduct security screening investigations and to counter sedition, treason and terrorist and -related activities;

(b) "crime intelligence", which means intelligence used in the prevention of crime or to conduct criminal investigations and to prepare evidence for the purpose of law enforcement and the prosecution of offenders;

(c) "departmental intelligence", which means intelligence about any threat or potential threat to the national security and stability of the Republic which falls within the functions of a department of State, and includes intelligence needed by such department in order to neutralise such a threat;

(d) "domestic intelligence", which means intelligence on any internal activity, factor or development which is detrimental to the national stability of the Republic, as well as threats or potential threats to the constitutional order of the Republic, the safety and the well-being of its people, on all matters relating to the advancement of public good and all matters relating to the protection and preservation of all things owned or maintained for the public by the State;

(e) "domestic military intelligence", which means intelligence required for the planning and conduct of military operations within the Republic to ensure security and stability for its people;

(f) "foreign intelligence", which means intelligence on any external threat or potential threat to the national interests of the Republic and its people, and intelligence regarding opportunities relevant to the protection and promotion of such national interests irrespective of whether or not it can be used in the formulation of the foreign policy of the Republic; and

(g) "foreign military intelligence", which means intelligence regarding the war potential and military establishment of foreign countries (including their capabilities, intentions, strategies and tactics) which can be used by the Republic in the planning of its military forces in time of peace and for the conduct of military operations in time of war;

"legitimate interest" means an interest that is consistent with the Constitution, applicable law and the mandate of an institution or organ of state;

"Minister" means the President or the member of the Cabinet designated by the President in terms of section 209(2) of the Constitution to assume political responsibility for the control and direction of the intelligence services established in terms of section 209(1) 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 structures" means—

(a) the National Intelligence Coordinating Committee (Nicoc);

(b) the intelligence division of the National Defence Force;

(c) the intelligence division the South African Police Service; and

(d) the Agency;

"national interest of the Republic" has the meaning assigned to it in section 11;

"national security" means the resolve of South Africans as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life, and includes protection of the people and occupants of the Republic from hostile acts of foreign intervention, terrorist and related activities, espionage and violence, whether directed from or committed within the Republic or not, and includes the carrying out of the Republic's responsibilities to any foreign country in relation to any of the matters referred to in this definition;

"need-to-know" means a determination made by an authorised person that a person with a valid security clearance gains access to such classified information as may be necessary to enable him or her to perform his or her functions;

"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, 2003 (Act No.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 the organ of state that authorised the original classification, or the person or entity authorised by the head of the organ of state to do so;

"personal information" means any information concerning an identifiable natural person which, if disclosed, could reasonably be expected to endanger the life or physical safety or general welfare of an individual;

"physical security" means the use of physical measures to—

(a) prevent or deter unauthorised persons from accessing protected information;

(b) detect attempted or actual unauthorised access; and

(c) activate an appropriate response;

"Promotion of Access to Information Act" means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

"protected information" means State information which requires protection against destruction, loss or unlawful 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" includes regulations issued by the Minister in terms of this Act;
"secret information" has the meaning assigned to it in section 15(2);
"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 the main functions or structures of an institution, charged with overseeing the development, implementation and maintenance of the institution's security policy;
"sensitive information" means information which must be protected from unlawful disclosure in order to prevent the national interest of the Republic from being harmed;
"State information" means information generated, acquired or received by organs of state or in the possession or control of organs of state;
"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;
"State security matter" includes any matter which is dealt with by the Agency or which relates to the functions of the Agency or to the relationship existing between any person and the Agency;
"technical surveillance countermeasures" means the process involved in the detection, localisation, identification and neutralisation of technical surveillance of an individual, an institution, a facility or a vehicle;
"this Act" includes regulations made in terms of section 48;
"top secret information" has the meaning assigned to it in section 15(3);
"valuable information" means—

(a) the information that should be retained for later use or reference; and
(b) that the alteration, loss or destruction of such information is likely to—
  (i) impede or frustrate the State in the conduct of its functions; and
  (ii) deny the public or individuals of a service or benefit to which they are entitled.

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

(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.

(4) For the purposes of this Act a person is regarded as having knowledge of a fact if—

(a) that person has actual knowledge of the fact; or
(b) the court is satisfied that—
  (i) the person believes that there is a reasonable possibility of the existence of that fact; and
  (ii) the person has failed to obtain information to confirm the existence of that fact,

and "knowing" shall be construed accordingly.

(5) For the purposes of this Act a person ought reasonably to have known or suspected a fact if the conclusions that he or she ought to have reached, are those which would have been reached by a reasonably diligent and vigilant person having both—

(a) the general knowledge, skill, training and experience that may reasonably be expected of a person in his or her position; and
(b) the general knowledge, skill, training and experience that he or she in fact has.

(6) In regard to minimum sentences as provided for in sections 32, 33, 34, 35, 36, 38, 39, 40 and 43 of this Act, if a court is satisfied that substantial and compelling circumstances exist which justify the imposition of a lesser sentence than the sentence prescribed in that section, it shall enter those circumstances on the record of the proceedings, and must thereupon impose such lesser sentence.

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 recognising 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 which 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 unlawful disclosure;

(g) provide for the classification and the declassification of classified information;

(h) create a system for the review of the status of classified information by way of regular reviews and requests for review;

(i) regulate the accessibility of declassified information to the public;

(j) harmonise the implementation of this Act with the Promotion of Access to Information Act, 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) criminalise 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 applies 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 8;

(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;

(c) grant to an organ of state an extension of the 18 months' period referred to in section 23(5);

(d) exempt an organ of state from declassifying information before such information is transferred to the National Archives or other archives in terms of section 26; or

(e) exempt an organ of state from section 30(1) insofar as the section authorises the Agency to carry out on-site inspections and reviews for the purposes of monitoring the protection of information programmes.

(3) The Minister, on his or her own accord or on a request made by an organ of state, may 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.

CHAPTER 2

GENERAL PRINCIPLES OF STATE INFORMATION

State information

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

Protected information

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

(2) State information in material or documented form which requires protection against unlawful 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

6. 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 and 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, to bring criminals to justice, to protect the national security and to engage in effective government and diplomacy;

(h) measures to protect State 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 taken in terms of this Act must—

(i) have regard to the freedom of expression, the right of access to information 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;

(j) paragraphs *(a)* to *(i)* are subject to the security of the Republic, in that the national security of the Republic may not be compromised.

CHAPTER 3

NATIONAL INFORMATION SECURITY STANDARDS AND DEPARTMENTAL POLICIES AND PROCEDURES

National standards and procedures

7. (1) The Minister must, within 12 months of the commencement of this Act—

(a) prescribe broad categories and subcategories of information that may be classified, downgraded and declassified and protected against destruction, alteration and loss;

(b) prescribe categories and subcategories of information that may not be protected in terms of this Act; and

(c) prescribe national information security standards and procedures for the categorisation, classification, downgrading and declassification of information.

(2) The national information security standards referred to in subsection (1)*(b)* include, but are not limited to—

(a) organisation 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 Police; and

(e) continuity planning.

(3) Before the Minister prescribes any categories of information in terms of subsection (1)*(a)*, the Minister—

(a) must by notice in the *Gazette* provide an opportunity for organs of state and other interested persons to submit comments in respect of the categorisation in question; and

(b) may take into account any comments received as a result of the notice contemplated in paragraph *(a)*.

(4) Subsection (2) applies to any modification to the categories of information prescribed in terms of subsection (1).

(5) No measure taken under this section may impede or prevent the National Archives or any other archive from 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

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

(2) Departmental policies and directives must not be inconsistent with the national information security standards prescribed in terms of section 7.

(3) Each organ of state must establish departmental policies, directives and categories in terms of subsection (1) within 18 months of the commencement of this Act.

CHAPTER 4

INFORMATION WHICH REQUIRES PROTECTION AGAINST ALTERATION, DESTRUCTION OR LOSS

Process of determining information as valuable

9. (1) State information must be determined as valuable when that information is identified in terms of a prescribed procedure or policy as information that should be protected from destruction and loss.

(2) Items of valuable information and files, integral file blocks, file series or categories of valuable information must be entered into a departmental register of valuable information.

(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 categorised as valuable, all individual items of information that fall within a valuable category are automatically deemed to be valuable.

Protection of valuable information

10. (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 National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996).

CHAPTER 5

INFORMATION WHICH REQUIRES PROTECTION AGAINST DISCLOSURE

Part A

Sensitive Information

National interest of Republic

11. (1) The national interest of the Republic includes, but is not limited to—

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

(b) 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 includes—

(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 the Republic 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 the Republic's stability, security, integrity and development; and

(g) all matters that are subject to mandatory protection in terms of sections 34 to 42 of the Promotion of Access to Information Act, whether in classified form or not.

(4) The determination of what is in the national interest of the Republic must at all times be guided by the values referred to in section 1 of the Constitution.

Part B

Commercial information

Nature of commercial information

12. (1) Commercial information becomes the subject matter of possible protection from disclosure under the following circumstances:

(a) Commercial information of an organ of state or information 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 organ of state, organisation or individual concerned;

(b) information that could endanger the national interest of the Republic.

(2) 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, styles of work, apparatus, and the identity, amount or source of income, profits, losses or expenditures of any person, firm, partnership, corporation or association.

(3) Only commercial information which the State is not otherwise authorised by law to release may be protected against disclosure.

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

CHAPTER 6

CLASSIFICATION AND DECLASSIFICATION OF INFORMATION

Part A

Classification

Nature of classified information

13. Classified information—

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

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

(c) may be made accessible only to those holding an appropriate security clearance and who have a legitimate need to access the information in order to fulfil their official duties or contractual responsibilities;

(d) is considered to be valuable information that must be protected against destruction and loss; and

(e) must be classified in terms of section 15.

Method of classifying information

14. (1) State information is classified by the relevant classification authority in terms of section 17 when—

(a) a classification authority has identified information in terms 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 and all individual items of information that fall within such a classified file, integral file block, file series or category are considered to be classified.

(3) The classification of information is determined through a consideration of the directions as contained in section 17.

Classification levels

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

(a) sensitive information, the unlawful disclosure of which may be harmful to the security or national interest of the Republic 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 national interest of the Republic or could jeopardise the international relations of the Republic;

(b) commercial information, the disclosure of which may cause serious financial loss to an entity; 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 national interest of the Republic or may cause other states to sever diplomatic relations with the Republic;

(b) commercial information, the disclosure of which may—
  (i) have disastrous results with regard to the future existence of an entity; or
  (ii) cause serious and irreparable harm to the security or interests of the State;
(c) personal information the disclosure of which may endanger the life of the individual concerned.

Authority to classify information

16. (1) Any head of an organ of state may classify or reclassify information using the classification levels set out in section 15.

(2) A head of an organ of state may delegate in writing authority to classify information to a subordinate staff member.

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

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

(5) Items, files, integral file blocks, file series or categories of State information may be determined in the manner contemplated in subsection (1) as classified in advance, but only by a head of an organ of state.

(6) When State information is categorised as classified, all individual items of information that fall within a classified category are automatically regarded as classified.

Directions for classification

17. (1) For the purposes of classification, classification decisions must be guided by section 21 and the following:
(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 embarassment to a person, organisation, 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 conducted strictly in accordance with sections 11 and 15;
(d) information is classified only when there is—
  (i) a clear, justifiable and legitimate need to do so; and
  (ii) a demonstrable need to protect the information in the national interests;
(e) if there is significant doubt as to whether information requires protection, the matter must be referred to the Minister for a decision;
(f) the decision to classify information must be based solely on the guidelines and criteria set out in this Act, the policies and regulations 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 may not be based on any extraneous or irrelevant reason;
(i) classification decisions ought to be assessed and weighed against the benefits of secrecy, taking into account the following factors:
  (i) The vulnerability of the information;
  (ii) the threat of damage from its disclosure;
  (iii) the risk of loss of the information;
  (iv) the value of the information to adversaries;
  (v) the cost of protecting the information; and
  (vi) the 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*) classification must 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.

(2) The application of the classification principles may not in any way inhibit or prevent officials from informing authorised officials of such information in order to fulfil law enforcement or intelligence functions authorised or prescribed by law.

Report and return of classified records

18. A person who is in possession of a classified record knowing that such record has been unlawfully communicated, delivered or made available other than in the manner and for the purposes contemplated in this Act, except where such possession is for any purpose and in any manner authorised by law, must report such possession and return such record to a member of the South African Police Service or the Agency.

Part B

Declassification

Authority to declassify information

19. (1) The organ of state that classified information is responsible for its declassification and downgrading.

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

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

(4) The Agency is 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 Agency must 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 and all individual items of information that fall within such a declassified category are considered to be declassified.

Maximum protection periods

20. In accordance with section 11(2) of the National Archives of South Africa Act, 1996 (Act No. 43 of 1996), information may not remain classified for longer 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, that the continued protection of the information from unlawful disclosure is—

(*a*) crucial to the safeguarding of the national security of the Republic;

(*b*) necessary to prevent significant and demonstrable damage to the national interest; or

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

CHAPTER 7

CRITERIA FOR CONTINUED CLASSIFICATION OF INFORMATION

Continued classification of information

21. (1) In taking a decision whether or not to continue the classification of information, the head of an organ of state must consider whether 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 investigative method, or reveal the identity of an intelligence or police source when the unlawful disclosure of that source would clearly and demonstrably damage the national interests of the Republic or the interests of the source or his or her family;

(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 authorised;

(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 the Republic;

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

(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.

(3) The Minister may, after taking into consideration all aspects as indicated in subsection (2), section 11 and section 17(1)*(i)*, authorise the classification or declassification of any category or class of classified information.

Regular reviews of classified information

22. (1) At least once every 10 years, the head of an organ of state must review the classified status of all classified information held or possessed in that organ of state.

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

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

(4) When conducting a review, the head of an organ of state must apply the criteria for the continued classification of information contemplated in this Chapter.

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

Request for status review of classified information

23. (1) A request for the declassification of classified information may be submitted to the head of an organ of state by an interested non-governmental party or person.

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

(3) In conducting such a review the head of an organ of state must take into account the considerations for the continued classification of information as contemplated in this Chapter.

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

(a) develop procedures to process requests for the review of the classified 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 25.

(5) The procedures referred to in subsection (4)*(a)* must be implemented within 18 months of the date on which this Act takes effect.

(6) In response to a request for the review of the classified status of information in terms of this Act the head of 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 as top secret.

Status review procedure

24. (1) A request for a review of the classified status of information must describe the document or materials containing the information or describe the category or subject matter of information with sufficient clarity to enable the head of an organ of state to locate it with ease.

(2) The head of an organ of state receiving a request in the prescribed manner for a review of the status of classified information must make a determination and in the case of a refusal provide reasons within 90 days of the date of receipt of such request.

Appeal procedure

25. (1) If the head of an organ of state denies a request for declassification or the lifting of the 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) Any appeal referred to in subsection (1) must be lodged within 30 days of receipt of the decision and reasons therefor.

(3) Upon receipt of an appeal, the Minister of an organ of state must make a finding and in the case of refusal provide reasons within 90 days of the date of receipt of such request.

CHAPTER 8

TRANSFER OF RECORDS TO NATIONAL ARCHIVES

Transfer of public records to National Archives

26. (1) The head of an organ of state must review the classification of information before it is transferred to the National Archives or other archives established by law.

(2) At the date on which this Act takes effect, public records, including records marked classified that are transferred to the National Archives or other archives, are considered to be automatically declassified.

(3) The head of an organ of state that holds classified records that originated in another organ of state must—

(a) notify the originating organ of state before transferring classified records to the National Archives or other archives; and

(b) 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, are 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, classified records in possession of the National Archives or other archives are regarded as being automatically declassified at the expiry of the relevant protection periods referred to in section 20.

(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 9

RELEASE OF DECLASSIFIED INFORMATION TO PUBLIC

Release of declassified information to public

27. (1) Classified information that is declassified, may be made available to the public in accordance with this Act, the Promotion of Access to Information Act or any other law.

(2) Unless ordered by a court, no classified information may be made available 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 by another organ of state, it must refer the request and the pertinent records to that other organ of state for processing and may, after consultation with the other organ of state, inform the 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 29.

Request for classified information in terms of Promotion of Access to Information Act

28. (1) A request for access to a classified record that is made in terms of the Promotion of Access to Information Act must be dealt with in terms of that Act.

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

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

(4) If the refusal to grant access to a classified record is 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 National Declassification Database

29. (1) The National Archives and Records Services of South Africa must, in conjunction with those organs of state that originate classified information, establish a national declassification database.

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

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

(4) Every head of an organ of state must cooperate fully with the National Archives and Record Services of South Africa in the establishment and ongoing operations of the National Declassification Database.

(5) The Department of Defence Archive Repository referred to in section 83(3) of the Defence Act, 2002 (Act No. 42 of 2002), is part of the National Declassification Database.

(6) Information contained within the National Declassification Database must, at a reasonable fee, be made available and accessible to members of the public.

(7) 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.

CHAPTER 10

IMPLEMENTATION AND MONITORING

Responsibilities of Agency

30. (1) The Agency is responsible for ensuring implementation of protection of information practices and programmes in terms of this Act in all organs of state and government entities, including—

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

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

(c) provision of expert support and advice to—

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

(ii) Ministers who require assistance in the determination of appeals in terms of section 25; and

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

(2) The Agency must provide the following guidance and support to organs of State, excluding the South African Police Service and the South African National Defence Force:

(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 to organs of State which require assistance in the—

(i) classification and declassification of information; and

(ii) carrying out of regular reviews of classified information;

(d) identification and exploration of best departmental practices;

(e) development of education materials and the 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

(h) supplying of annual reports to the Minister.

Dispute resolution

31. If disputes arise between the Agency and any organ of State, the head of an organ of State concerned or the Agency may refer the matter to the Minister for resolution of the dispute.

CHAPTER 11

OFFENCES AND PENALTIES

Espionage offences

32. (1) It is an offence punishable on conviction by imprisonment for a period not less than 15 years but not exceeding 25 years, subject to section 1(6)—

(a) to unlawfully communicate, deliver or make available State information classified top secret which an offender knows or ought reasonably to have known or suspected would directly or indirectly benefit another State; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing State information classified top secret which an offender knows or ought reasonably to have known or suspected would directly or indirectly benefit another State.

(2) It is an offence punishable on conviction by imprisonment for a period not less than 10 years but not exceeding 15 years, subject to section 1(6)—

(a) to unlawfully communicate, deliver or make available State information classified secret which an offender knows or ought reasonably to have known or suspected would directly or indirectly benefit another State; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing State information classified secret which an offender knows or ought reasonably to have known or suspected will directly benefit another State.

(3) It is an offence punishable on conviction by imprisonment for a period not less than three years but not exceeding five years, subject to section 1(6)—

(a) to unlawfully communicate, deliver or make available State information classified confidential which an offender knows or ought reasonably to have known or suspected would directly or indirectly benefit another State; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing State information classified confidential which an offender knows or ought reasonably to have known or suspected would directly or indirectly benefit another state.

Hostile activity offences

33. (1) It is an offence punishable on conviction by imprisonment for a period not less than 15 years but not exceeding 25 years, subject to section 1(6)—

(a) to unlawfully communicate, deliver or make available State information classified top secret which an offender knows or ought reasonably to have known or suspected would directly or indirectly prejudice the State; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing State information classified top secret which an offender knows or ought reasonably to have known or suspected would directly or indirectly prejudice the State.

(2) It is an offence punishable on conviction by imprisonment for a period not less than 10 years but not exceeding 15 years, subject to section 1(6)—

(a) to unlawfully communicate, deliver or make available State information classified secret which an offender knows or ought reasonably to have known or suspected would directly or indirectly prejudice the State; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing State information classified secret which an offender knows or ought reasonably to have known or suspected would directly or indirectly prejudice the State.

(3) It is an offence punishable on conviction by imprisonment for a period not less than three years but not exceeding five years, subject to section 1(6)—

(a) to unlawfully communicate, deliver or make available State information classified confidential which an offender knows or ought reasonably to have known or suspected would directly or indirectly prejudice the State; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing State information classified confidential which an offender knows or ought reasonably to have known or suspected would directly or indirectly prejudice the State.

Harbouring or concealing persons

34. Any person who harbours or conceals a person whom he or she knows, or has reasonable grounds to believe or suspect, has committed, or is about to commit, an offence contemplated in section 32 or 33, is guilty of an offence and liable on conviction to imprisonment for a period not less than five years but not exceeding 10 years, subject to section 1(6).

Interception of or interference with classified information

35. (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 less than five years but not exceeding 10 years, subject to section 1(6).

(2) Any 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 on conviction to imprisonment for a period not less than five years but not exceeding 10 years, subject to section 1(6).

(3) Any 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 purposes of contravening this section, is guilty of an offence and liable on conviction to imprisonment for a period not less than five years but not exceeding 10 years, subject to section 1(6).

(4) Any person who utilises 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 on conviction to imprisonment for a period not less than five years but not exceeding 10 years, subject to section 1(6).

(5) Any person who contravenes any provision of 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 commits an offence and is liable on conviction to imprisonment for a period not less than five years but not exceeding 10 years, subject to section 1(6).

(6) *(a)* Without derogating from the generality of subsection (6)*(b)*—

"access to a computer" includes access by whatever means to any program or data contained in the random access memory of a computer or stored by any computer on any storage medium, whether such storage medium is physically attached to the computer or not, where such storage medium belongs to or is under control of the State;

"content of any computer" includes the physical components of any computer as well as any program or data contained in the random access memory of a computer or stored by any computer on any storage medium, whether such storage medium is physically attached to the computer or not, where such storage medium belongs to or is under the control of the State;

"modification" includes both a modification of a temporary or permanent nature; and

"unauthorised access" includes access by a person who is authorised to use the computer but is not authorised to gain access to a certain program or to certain data held in such computer or is not authorised, at the time when the access is gained, to gain access to such computer, programme or data.

(b) Any person who wilfully gains unauthorised access to any computer which belongs to or is under the control of the State or to any program or data held in such a computer, or in a computer to which only certain or all employees have restricted or unrestricted access in their capacity as employees of the State, is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.

(c) Any person who wilfully causes a computer which belongs to or is under the control of the State or to which only certain or all employees have restricted or unrestricted access in their capacity as employees to perform a function while such person is not authorised to cause such computer to perform such function, is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.

(d) Any person who wilfully performs an act which causes an unauthorised modification of the contents of any computer which belongs to or is under the control of the State or to which only certain or all employees have restricted or unrestricted access in their capacity as employees of the State with the intention to—

(i) impair the operation of any computer or of any program in any computer or of the operating system of any computer the reliability of data held in such computer; or

(ii) prevent or hinder access to any program or data held in any computer,

is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not less than three years but not exceeding five years, subject to section 1(6).

(e) Any act or event for which proof is required for a conviction of an offence in terms of this subsection which was committed or took place outside the Republic is deemed to have been committed or have taken place in the Republic: Provided that—

(i) the accused was in the Republic at the time he or she performed the act or any part thereof by means of which he or she gained or attempted to gain unauthorised access to the computer, caused the computer to perform a function or modified or attempted to modify its content;

(ii) the computer by means of or with regard to which the offence was committed, was in the Republic at the time the accused performed the act or any part thereof by means of which he or she gained or attempted to gain unauthorised access to it, caused it to perform a function or modified or attempted to modify its contents; or

(iii) the accused was a South African citizen at the time of the commission of the offence.

Registration of intelligence agents and related offences

36. (1) Any person who is in the Republic and who is—

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

(b) not employed or operating as an agent 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 Agency.

(2) Any person who fails to register as an intelligence or security agent in accordance with this section is guilty of an offence and liable on conviction to imprisonment for a period not less than three years but not exceeding five years, subject to section 1(6).

Attempt, conspiracy and inducing another person to commit offence

37. 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, is 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 classified and related information

38. Any person who discloses classified information or information referred to in section 11(3)*(g)* outside of the manner and purposes of this Act, except where such disclosure is for a purpose and in a manner authorised by law, is guilty of an offence and liable on conviction to imprisonment for a period not less than three years but not exceeding five years, subject to section 1(6).

Failure to report possession of classified information

39. Any person who fails to comply with section 18 is guilty of an offence and liable to a fine or imprisonment for a period not less than three years but not exceeding five years or to both such fine and imprisonment, subject to section 1(6).

Provision of false information to national intelligence structure

40. Any person who provides information to a national intelligence structure that is false or fabricated, knowing that it is false or has been fabricated, is guilty of an offence and liable on conviction to imprisonment for a period not less than three years but not exceeding five years, subject to section 1(6).

Destruction or alteration of valuable information

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

Improper classification

42. Any person who knowingly classifies information in order to achieve any purpose ulterior to this Act, including the classification of information in order to—

(a) conceal breaches of the law;

(b) promote or further an unlawful act, inefficiency or administrative error;

(c) prevent embarrassment to a person, organisation or agency; or

(d) give undue advantage to anyone within a competitive bidding process,

is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding three years.

Prohibition of disclosure of State security matter

43. (1) Any person who has in his or her possession or under his or her control or at his or her disposal information which he or she knows or reasonably should know is a State security matter, and who—

(a) discloses such information to any person other than a person to whom he or she is authorised to disclose it or to whom it may lawfully be disclosed;

(b) publishes or uses such information in any manner or for any purpose which is prejudicial to the security or interests of the State;

(c) retains such information when he or she has no right to retain it or when it is contrary to his or her duty to retain it, or neglects of fails to comply with any

directions issued by lawful authority with regard to the return of disposal thereof; or

(d) neglects or fails to take proper care of such information, or so to conduct himself or herself as not to endanger the safety thereof,

is guilty of an offence and liable on conviction to imprisonment for a period not less than five years but not exceeding 10 years, subject to section 1(6), or, if it is proved that the publication of disclosure of such information took place for the purpose of its being disclosed to a foreign state to imprisonment, for a period not less than 10 years but not exceeding 15 years, subject to section 1(6).

Extra-territorial application of Act

44. 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 must be regarded as having been committed in the Republic.

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

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

CHAPTER 12

PROTECTION OF INFORMATION IN COURTS

Protection of State information before courts

46. (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, and upon considering issues of national security, national interest of the Republic as referred to in section 11 and any other law, orders full or limited disclosure, with or without conditions.

(2) Unless a court orders the disclosure of classified information or orders the limited or conditional disclosure of classified information, the court must issue directions for the proper protection of such information during the course of legal proceedings, which may include, but are not limited to—

(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 or alternatively to obtain the submissions of the Director-General of the Agency.

(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 subsection (1) must be held *in camera*, and any person not authorised to receive such information may not attend such hearings unless authorised by a court.

(5) A court may, if it considers it 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 or the Director-General of the Agency, as the case may be, in consultation with the Minister, must declassify information required in legal proceedings, either in whole or in part, unless it is strictly necessary to maintain the classification in terms of this Act.

(7) In addition to the measures set out in this section, a court in criminal proceedings has the same powers as those conferred upon a court under section 154(1) and (4) of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), and the said section applies with the necessary changes.

(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, is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 10 years.

(9) *(a)* 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 publicly disclosed or published, may undermine the national interest.

(b) A court hearing such an application may determine its own procedures and may impose limitations on the disclosure of the information in question, pending its decision.

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

(11) At any court hearing relating to this Act it is mandatory that a minimum of three judicial officers preside over the matter.

CHAPTER 13

GENERAL PROVISIONS

Reports

47. (1) Each head of an organ of state must, by no later than 31 December of each year, submit a report to his or her Minister, and forward a copy of such report to the Minister and the Agency, 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.

(2) The Agency must 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 Agency must report annually to Parliament on the monitoring carried out in terms of this Act and on the status of the protection of information practices by all organs of state.

(4) When the Agency submits its report to Parliament, the Agency must forward copies of the report to every head of an organ of state.

Regulations

48. (1) The Minister may make regulations consistent with this Act regarding—

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

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

(c) training and guidance to be supplied to State employees in respect of their responsibilities to ensure that valuable and classified information are adequately protected;

(d) the organisation 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 of information, including training and guidance to be supplied to staff members on how to classify information and how to prevent the over-classification of information;

(j) the roles of any national intelligence structures with regard to the protection of information;

(k) the reporting of security breaches at any organ 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 prescribed in terms of section 7(1)*(b)* and *(c)*.

(2) The Minister must make the regulations referred to in subsection (1) within 18 months of the date on which this Act takes effect.

Transitional provisions

49. (1) The provisions of this Act are suspended from operation pending the establishment of the standards, policies and procedures contemplated in Chapter 3 and the regulations contemplated in section 48, or for a period of 18 months from the date on which this Act takes effect, whichever occurs first, except—

(a) Chapter 3;

(b) section 18, which provides for the reporting and return of classified records;

(c) section 27, which provides for the release of declassified information to the public;

(d) section 28, which provides for requests for access to classified information in terms of the Promotion of Access to Information Act;

(e) section 29, which provides for the establishment of the National Declassification Database;

(f) Chapter 10, which sets out the responsibilities of the Agency;

(g) section 48, which provides for the making of regulations;

(h) the definitions and principles which give effect to the sections referred to in paragraphs *(a)* to *(g)*; and

(i) Chapter 13.

(2) During the period contemplated in subsection (1) the following provisions of this Act apply to the implementation and interpretation of the MISS Guidelines:

(a) The general principles of State information set out in section 6; and

(b) the principles of classification set out in section 17.

Repeal of laws

50. (1) Subject to section 49, the Protection of Information Act, 1982 (Act No. 84 of 1982), is hereby repealed.

(2) Section 83(3)*(c)* of the Defence Act, 2002 (Act No. 42 of 2002), is repealed.

Short title and commencement

51. This Act is called the Protection of Information Act, 2010, and comes into operation on a date fixed by the President by proclamation in the *Gazette*.

MEMORANDUM ON THE OBJECTS OF THE PROTECTION OF INFORMATION BILL

1. BACKGROUND

1.1 The Protection of Information Bill (the Bill) will ensure a coherent approach to protection of State information and the classification and declassification of State information and will create a legislative framework for the State to respond to espionage and other associated hostile activities.

1.2 The Bill sets out procedures on how classified documents are to be handled during court proceedings, and requires courts to prevent public disclosure of classified documents that form part of court records.

2. OBJECTS OF BILL

2.1 The Bill seeks to—

(a) create a statutory framework for the protection of State information. State information is information generated by organs of state or is in the possession or control of organs of state;

(b) set out criteria and processes in terms of which State information may be protected from destruction or from unlawful disclosure;

(c) set out criteria and processes in terms of which information which is protected from disclosure and which is classified, may be declassified;

(d) create offences and proposed sentences for unlawful disclosure of information, including the crime of espionage;

(e) make it an offence for an individual to knowingly supply false information to the national intelligence structures;

(f) establish guidelines for the treatment by courts of classified documents;

(g) provide for the Minister of State Security to issue regulations on information security across government; and

(h) repeal the existing Protection of Information Act (Act No. 84 of 1982).

2.2 **Structure of Bill**

(a) **Chapter 1: Definitions, objects and application of the Bill**

This chapter provides detailed definitions of all technical terms and concepts. The statute will apply to all organs of state and natural and juristic persons. The Minister of State Security may, on good cause shown, exempt organs of state from certain provisions of the Act.

(b) **Chapter 2: General principles of information**

This chapter outlines the principles which underpin the Act and which inform its implementation and interpretation.

(c) **Chapter 3: National information security standards and departmental policies and procedures**

Within 12 months of the date on which this Act comes to effect, the Minister of State Security must issue national information security standards prescribing broad categories of information that may be protected (classified or protected against destruction, alteration or loss). This chapter sets out what matters such standards may cover.

(d) **Chapter 4: Information that requires protection against alteration, destruction or loss**

This chapter sets out what information may be protected against alteration, destruction or loss (known as "valuable information"); the process of determining information as valuable; and how such information is to be protected.

(e) **Chapter 5: Information which requires protection against disclosure**

This chapter sets out what information may be protected from unlawful disclosure, and divides such information into two categories: **"sensitive"** and **"commercial"**.

(f) **Chapter 6: Classification of information**

This chapter sets out principles that must be observed when classifying information; and outlines the method of classifying information. It also describes the three levels of classification: confidential, secret and top secret; and specifies who has the authority to classify information. Sensitive, commercial or personal information which is in material form may be protected by way of classification. Information may not remain classified for more than 20 years unless the head of the organ of state that classified the information certifies to the satisfaction of his or her Minister that continued protection against disclosure is critical to the national security of South Africa; necessary to prevent identifiable damage to the national interest; or necessary to prevent demonstrable physical or life-threatening harm to a person or persons.

(g) **Chapter 7: Criteria for continued classification of information**

This chapter outlines the criteria that a head of an organ of State must consider in reviewing the classified status of information. It further sets out the procedure in terms of which interested third parties may request the head of an organ of state to review the status of classified material. Heads of organs of state are required to review the status of classified information at least once every 10 years.

(h) **Chapter 8: Transfer of records to national archives**

Organs of State are required to review the status of information before transferring such information to the National Archives. Information transferred to the National Archives may not hold a classified status and shall be deemed to be automatically declassified. Existing classified information within the National Archives shall be subject to the declassification stipulations set out in the Act.

(i) **Chapter 9: Release of declassified information to public**

Information that is declassified may be made available to the public in accordance with applicable national and departmental policies. A request made in terms of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), for a classified record proceeds as determined in that Act. The classification must be reviewed and if it is decided that access is to be granted, the record must be declassified before it is made available. The National Archives 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. Information contained within the database shall, at a reasonable cost, be made available and accessible to members of the public.

(j) **Chapter 10: Implementation and Monitoring**

The Department of State Security shall have the responsibility to develop, coordinate and facilitate the implementation of national policies in an efficient and consistent manner across all organs of state. The responsibilities of this Department do not extend to the national intelligence structures such as the Department of Police and the Department of Defence and War Veterans given that these departments have the necessary capacity and competence to implement the provisions contained in the Act.

(k) **Chapter 11: Offences and penalties**

This chapter provides for the following offences: Espionage offences; hostile activity offences; harbouring or concealing persons involved in espionage or hostile activities; unauthorised access to, interception of or interference with classified information; registration of agents and related offences; attempt, conspiracy, and inducing another person to commit an offence; disclosure of classified and related information; knowing possession of classified information; destruction of valuable information; improper classification; disclosure of a State security matter. The penalties assigned vary on the basis of the nature of the offence and the actual or potential harm caused. This chapter further provides for the minimum sentences of offences.

(l) **Chapter 12: Protection of information before courts**

This chapter outlines the process to be adopted by courts in the handling of classified documents that form part of court records. All documents with a classification shall remain protected by courts unless the courts direct otherwise.

(m) **General provisions**

This chapter deals with the submission of reports by organs of state and the National Intelligence Agency; the issuing of regulations by the Minister of State Security; and the institution of certain transitional provisions. The provisions of the Act are suspended pending the establishment of the standards, policies and procedures and the regulations, or for a period of 18 months from the commencement of the Act, whichever occurs first, with the exception of several identified sections.

3. DEPARTMENTS OR BODIES CONSULTED

A draft Bill was distributed to the Department of Police, the Department of Justice and Constitutional Development and the Department of Defence and War Veterans for comments.

4. FINANCIAL IMPLICATIONS FOR THE STATE

None.

5. PARLIAMENTARY PROCEDURE

5.1 The State Law Advisers and the Ministry of State Security are of the opinion that this Bill must be dealt with in accordance with the procedure established by section 75 of the Constitution since it contains no provision to which the procedure set out in section 74 or 76 of the Constitution applies.

5.2 The State Law Advisers are of the opinion that it is not necessary to refer this Bill to the National House of Traditional Leaders in terms of section 18(1)*(a)* of the Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003), since it does not contain provisions pertaining to customary law or customs of traditional communities.