REPUBLIC OF SOUTH AFRICA

PROTECTION OF STATE INFORMATION BILL

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

(MINISTER OF STATE SECURITY)

[B6 —2010]

02 September 2011

BILL

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

PREAMBLE

Recognising that national security is subject to the authority of Parliament and the national executive, as contemplated in Section 198 of the Constitution;

Mindful of the right of access to any information held by the State provided for in Section 32 of the Constitution;

Acknowledging that the right of access to any information held by the State may be restricted when necessary for reasons of national security;

Recognising the harm caused by excessive secrecy;

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

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 10

IMPLEMENTATION AND MONITORING

CHAPTER 11

OFFENCES AND PENALTIES

CHAPTER 12

PROTECTION OF STATE INFORMATION IN COURTS

CHAPTER 13

GENERAL PROVISIONS

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 contemplated in Schedule 1 to the Public Service Act, 1994 (Act No. 103 of 1994), and includes the National Intelligence Agency, South African Secret Service, Electronic Communications Security (Pty)Ltd (COMSEC), and the South African National Academy for Intelligence;

"archive" means the national archive or any archive established in terms of a provincial law and includes an archive kept by an organ of state;

"categorisation of state information" means the process by which state information is placed into categories for purposes of classifying such information and for purposes of declassification, downgrading and the lifting of the status of state 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 state information" means a process used to determine—

(a) the manner in which such state information may be classified in terms of sections 12 and 14; and

(b) the level of protection assigned to such state information;

"classified information" means state information that has been classified under this Act;

"**Classification Review Panel**" means the Panel established under section 20;

"confidential information" has the meaning assigned to it in section 12(1);

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

"declassification authority' means the entity or person authorised under section 16 to declassify classified information;

"declassification of state information" means the authorised change in the status of state 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 state information" means a change of classification of state information from its existing level to a lower level;

"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 1980, (Act No. 102 of 1980), the owner of the national key point;

"hostile activity" means —

(a) aggression against the Republic ;

(b) sabotage or terrorism aimed at the people of the Republic or a strategic asset of the Republic, whether inside or outside the Republic;

(c) an activity aimed at changing the constitutional order of the Republic by the use of force or violence; or

(d) a foreign or hostile intelligence operation;

" information" means any information contained in any document whether written, copied, drawn, painted, printed, filmed, photographed, magnetic, optical, digital, electronic or any other type of recording, measure, procedure, object or verbal announcement;

" 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 peddling" means the conduct referred to in section 45;

"information security" means the safeguarding or protection of state information in whatever form;

"intelligence" means the process of gathering, evaluation, correlation and interpretation of security information, including activities related thereto;

"Minister" means 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 security" includes the protection of the people of the Republic and the territorial integrity of the Republic against—

(a) the threat of use of force or the use of force;

(b) the following acts:

(i) hostile acts of foreign intervention directed at undermining the constitutional order of the Republic;

(ii) terrorism or terrorist related activities;

(iii) espionage;

(iv) exposure of a State security matter with the intention of undermining the constitutional order of the Republic;

(v) exposure of economic, scientific or technological secrets vital to the Republic;

(vi) sabotage; and

(vii) serious violence directed at overthrowing the constitutional order of the Republic;

(c) acts directed at undermining the capacity of the Republic to respond to the use of, or the threat of the use of, force and carrying out of the Republic's responsibilities to any foreign country and international organisations in relation to any of the matters referred to in this definition, whether directed from, or committed within, the Republic or not,

but does not include lawful political activity, advocacy, protest or dissent;

"non state actor" means any person or entity other than a state engaged in a hostile activity;

"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 classification authority that authorised the original classification;

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

"prescribed" means prescribed by regulation made in terms of section 54;

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

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

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

"regulations" means the regulations issued by the Minister in terms of this Act;

"**Request for access** means a request for access contemplated in section 1 of the Promotion of Access to Information Act;

"**relevant Minister**" means any Cabinet member whose portfolio is affected by this Act;

"secret information" has the meaning assigned to it in section 12 (2);

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

"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 security 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 security matter" includes any matter, which has been classified in terms of this Act and, 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, facility or vehicle;

"this Act" includes regulations made in terms of section 54;

"top secret information" has the meaning assigned to it in section 12 (3);

"valuable information" means information contemplated in this Act whose unlawful alteration, destruction or loss is likely to 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) In respect of classified information and despite section 5 of the Promotion of Access to Information Act, this Act prevails if there is a conflict between a provision of this Act and provision of another Act of Parliament that regulates access to classified information.

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 security of the Republic;

(c) establish general principles in terms of which state information may be made available or accessible or 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 state information is safeguarded in terms of this Act;

(f) describe the nature and categories of state information that may be protected from destruction, loss or unlawful disclosure;

(g) regulate the conditions for 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 access to classified information and status review;

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

(j) to establish a Classification Review Panel to review and oversee status review, classification and declassification procedures;

[(j) **harmonise the implementation of this Act with the Promotion of Access to Information Act, 2000, and the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996);]**

(k) criminalise espionage and activities hostile to the Republic and provide for certain other offences and penalties; and

(l) repeal the Protection of Information Act, 1982 (Act No. 84 of 1982).

Application of Act

3. (1) The provisions of this Act with regard to the protection of valuable information against alteration, loss and destruction apply to all organs of state.

(2) The classification, reclassification and declassification provisions of this Act—

(a) apply to the security services of the Republic and the oversight bodies referred to in Chapter 11 of the Constitution; and

(b) may be made applicable by the Minister, on good cause shown, by publication in the Gazette, to any organ of state or part thereof that applies in the prescribed manner, to have those provisions apply to it.

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 that clearly sets out reasonable and objectively justified public or private considerations, state information should be available and accessible to all persons;

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

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

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

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

(f) accessible state 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 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) in balancing the legitimate interests referred to in paragraphs *(a)* - *(i)* the relevant Minister, a relevant official or a court must have due regard to the security of the Republic, in that the national security of the Republic may not be compromised.

CHAPTER 3

POLICIES AND PROCEDURES

Policies and procedures

7. (1) The head of each organ of state must where applicable

establish policies, directives and categories for classifying, downgrading and declassifying state information and protection against alteration, destruction and loss of state information created, acquired or received by that organ of state.

(2) Each organ of state must where applicable establish policies, directives and categories in terms of subsection (1) within six months of the date on which the regulations contemplated under section 54(4) are promulgated.

(3) Policies and directives must not be inconsistent with the national information security standards prescribed in terms of section 54.

CHAPTER 4

STATE INFORMATION WHICH REQUIRES PROTECTION AGAINST ALTERATION, DESTRUCTION OR LOSS

Process of determining state information as valuable

8. (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 against alteration, destruction and loss.

(2) 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

9. (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 prescribed

(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

CLASSIFICATION AND DECLASSIFICATION OF STATE INFORMATION

Part A

Classification

Nature of classified information

10. Classified information—

(a) is sensitive state information which is in material or record form;

(b) must be protected from unlawful disclosure and against alteration, destruction and loss as prescribed;

(c) must be safeguarded according to the degree of harm that could result from its unlawful disclosure;

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

(e) must be classified in terms of section 12 .

Method of classifying state information

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

(a) a classification authority has identified state information in terms of this Act as state information that warrants classification;

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

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

(2) The classification of state information is determined through a consideration of the conditions as contained in section 14.

Classification levels

12. (1) State information may be classified as Confidential if the information is sensitive information, the disclosure of which is likely or could reasonably be expected to cause demonstrable harm to national security of the Republic;

(2) State information may be classified as Secret if the information is sensitive information, the disclosure of which is likely or could reasonably be expected to cause serious demonstrable harm to national security of the Republic;

(3) State information may be classified as Top Secret

if the information is sensitive information, the disclosure of which is likely or could reasonably be expected to demonstrably cause serious or irreparable harm to the national security of the Republic.

Authority to classify state information

13. (1) Subject to Section 3, any head of an organ of state may classify or reclassify state information using the classification levels set out in section 12.

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

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

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

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

(6) Where a person is a member of Security Services as_contemplated in chapter 11 of the Constitution who by the nature of his or her work deals with state information that may fall within the ambit of this Act, that person must classify such information in accordance with the classification levels as set out in section 12.

(7) The member of the Security Services must submit the classified state information to the head of an organ of state in question for confirmation of the classification.

(8) The state information classified in terms of subsection (6) must remain classified until the head of an organ of state in question decides otherwise.

(9) The head of an organ of state retains accountability for any decisions taken in terms of a delegated authority contemplated in subsection (2).

Conditions for classification and declassification

14. (1) The decision to classify information must be based solely on the conditions set out in this Act.

(2) *(a)* Secrecy is justifiable only when necessary to protect national security;

(b) classification of state 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 state information in order to limit scrutiny and thereby avoid criticism;

(iii) prevent embarrassment to a person, organisation, or organ of state or agency;

(iv) unlawfully restrain or lessen competition; or

(v) prevent, delay or obstruct the release of state information that does not require protection under this Act;

(c) the classification of state information is an exceptional measure and should be conducted strictly in accordance with section 12;

(d) state 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 state information in the interest of national security;

(e) if there is significant doubt as to whether state information requires protection, the matter must be referred to the relevant Minister for a decision;

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

(g) classification decisions must balance openness against secrecy;

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

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

(j) classification must be in place only for as long as the protection is actually necessary; and

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

(3) Specific considerations with regard to the decision whether to classify state information 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 security 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; or

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

(4) The application of the classification conditions 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.

(5) When the conditions for classification contemplated in this section no longer exist state information must be declassified

Report and return of classified records

15. 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 to be dealt with in the prescribed manner.

Part B

Declassification

Authority to declassify state information

16. (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 a staff member at a sufficiently senior level 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) Subject to subsection (5), 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.

Maximum protection periods

17. 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 state information, certifies to the satisfaction of the Classification Review Panel that the conditions of classification set out in Section 12 and 14 still apply.

CHAPTER 6

REGULAR REVIEWS, REQUEST FOR ACCESS TO CLASSIFIED INFORMATION AND STATUS REVIEW

Regular reviews of classified information

18. (1) The head of an organ of state-

(a) must at least every 10 years review the classified status of all classified information held by that organ of state; or

(b) may review the classified status of classified information at any time but must do so at least once every 10-years.

(2) When conducting a review, the head of an organ of state must apply the conditions for the classification and declassification of state information set out in Sections 12 and 14.

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

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

(5) (a) The head of an organ of state must annually and in the prescribed manner prepare a report on the regular reviews conducted under this section by that organ of state and submit such report to the Classification Review Panel for certification.

(b) The classification Review Panel must table the report within 30 days of receipt thereof in Parliament if Parliament is in session, or if Parliament is not in session within 14 days after the commencement of the next Parliamentary session.

(c) The head of the organ of state must publish the annual report.

Request for access to classified information and status review

19. (1) If a request is made for access to information and it is established that the information requested is classified, that request must be referred to the relevant head of the organ of state for a review of the classification status of the state information requested in terms of the provisions of this Act.

(2) In conducting such a review the head of an organ of state must take into account the conditions for classification and declassification as set out in this chapter.

(3) (a) The head of the organ of state concerned must declassify the classified information in accordance with section 14 and grant the request for state information if that state information reveals evidence of -

(i) a substantial contravention of, or failure to comply with the law; or

(ii) an imminent and serious public safety or environmental risk; and

(b) the public interest in the disclosure of the state information clearly outweighs the harm that will arise from the disclosure.

(4) The head of the organ of state must –

(a) within 14 days of receipt of the request contemplated in subsection 3(a) (ii) grant the request for the declassification of classified information; or

(b) within 30 days, of receipt of the request contemplated in subsection (3) (a) (i) grant the request for the declassification of classified information.

(5) A court may condone non-observance of the time-period referred to in sub section (4) (a) on good cause shown where an urgent application is brought before court.

(6) If an application for a request referred to in subsection (1) is received, the head of the organ of state must within a reasonable time conduct a review of the classified information held by that organ of state relating to the request for declassification.

CHAPTER 7:

CLASSIFICATION REVIEW PANEL

Establishment of Classification Review Panel

20. (1) There is hereby established a Panel to be known as the Classification Review Panel.

(2) All organs of state must provide the Classification Review Panel such assistance as may be reasonably required for the effectiveness of the Classification Review Panel in the performance of its functions.

(3) (a) No organ of state or employee of an organ of state may interfere with, hinder or obstruct the Classification Review Panel or any member thereof or a person appointed under section 30 in the performance of its, his or her functions; and

(b) No access to classified information may be withheld from the Classification Review Panel on any ground.

Functions of Classification Review Panel

21. (1) The Classification Review Panel must—

(a) review and oversee status reviews, classifications and declassifications contemplated in this Act;

(b) receive all reports of 10 year reviews on the status of all classified information conducted by the organs of state; and

(c) receive, once a year, all reviews on status of classified information conducted by the organs of state during the course of a financial year.

(2) The Classification Review Panel may, with the concurrence of the Minister, make rules not in conflict with this Act for matters relating to the proper performance of the functions of the Classification Review Panel, including—

(a) time periods within which reports by the heads of organs of state must be submitted;

(b) state information to be supplied when a report is submitted;

(c) procedures regarding the deliberations and the conduct of work of the Panel; and

(d) random sampling methods to be employed in reviewing compliance under this Chapter.

Constitution and appointment of Classification Review Panel

22. (1) Due regard having been given to—

(a) participation by the public in the nomination process;

(b) transparency and openness; and

(c) the publication of a shortlist of candidates for appointment.

(2) The Joint Standing Committee on Intelligence must table a list of five persons for approval by the National Assembly.

(3) The National Assembly must by a resolution with a support of a majority vote of its members upon approval submit the list of five persons to the Minister for appointment.

(4) The Classification Review Panel is headed by a Chairperson who must either be an admitted attorney or advocate with at least ten years legal experience.

(5) The other four members of the Classification Review Panel must be suitably qualified of whom—

(a) at least one member must have expertise in the Constitution and the law;

(b) at least one member must have knowledge and experience of national security matters; and

(c) at least one member must have knowledge and experience of archive related matters.

(6) The members of the Classification Review Panel are appointed for a term of five years which term is renewable for one additional term only.

(7) A person may not be appointed as a member of the Classification Review Panel unless that person has a valid security clearance certificate issued under the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994).

Disqualification from membership

23. (1) A person may not be appointed as a member of the Classification Review Panel if he or she—

(a) is not a citizen of the Republic;

(b) is not resident in the Republic;

(c) is appointed by, or is in the service of, the state and receives remuneration for that appointment or service;

(d) is a member of Parliament, any provincial legislature or any municipal council;

(e) is an office-bearer or employee of any party, movement or organisation of a party-political nature;

(f) is an unrehabilitated insolvent;

(g) has been declared to be of unsound mind by a court of the Republic;

(h) has been convicted of an offence in the Republic, other than an offence committed prior to 10 May 1994 associated with political objectives, and was sentenced to imprisonment without an option of a fine.

(i) has been removed from an office of trust on account of misconduct involving theft or fraud.

Removal from office

24. (1) A member of the Classification Review Panel may be removed from the Panel on -

(a) the grounds of misconduct, incapacity or incompetence;

(b) a finding to that effect by the Joint Standing Committee on Intelligence; and

(c) the adoption by the Assembly of a resolution calling for that member's removal as member from the Classification Review Panel.

(2) A resolution of the National Assembly concerning the removal of a member from the Classification Review Panel must be adopted with a supporting vote of a majority of the members of the Assembly.

(3) The Minister—

(a) may suspend a member from the Classification Review Panel at any time after the start of the proceedings of a committee of the National Assembly for the removal of that person; and

(b) must remove a person from office upon adoption by the Assembly of the resolution calling for that person's removal.

(4) A member ceases to be a member of the Classification Review Panel if that member-

(a) resigns;

(b) fails to attend three consecutive meetings of the Classification Review Panel, unless his or her apology has been accepted; or

(c) becomes disqualified in terms of section 23.

(5) A vacancy in the Classification Review panel must be filled as soon as practicable in accordance with section 22.

Remuneration of members and staff

25. Members of the Classification Review Panel and staff of the Classification Review Panel must be paid such remuneration and allowances as determined by the Minister with the concurrence of the Minister of Finance.

Meetings of Classification Review Panel

26. (1) The Classification Review Panel meets as often as the circumstances require, but must meet at least once a month, at such times and places as the chairperson may determine.

(2) The Classification Review Panel may determine its own procedure for its meetings.

(3) The quorum for any meeting of the Classification Review Panel is three members.

(4) Any decision taken by the Classification Review Panel is not invalid merely by reason of a vacancy on the Panel provided that the required quorum is present at that meeting.

Decisions of Classification Review Panel

27. (1) The Classification Review Panel may confirm, vary or set aside any classification decision taken by the head of an organ of state and instruct the head of the organ of state concerned to change the classification status of the classified information, if necessary.

(2) The Classification Review Panel must before reaching a final decision afford the head of an organ of state an opportunity to respond in connection therewith, in any manner that may be expedient under the circumstances.

(3) A decision of the Classification Review Panel binds an organ of state subject to any appeal that the organ of state may lodge with a competent High Court.

Appointment of staff

28. (1) The Chairperson of the Classification Review Panel must appoint staff to assist the Panel in carrying out its functions.

(2) A person may not be appointed under subsection (1) unless that person has a valid security clearance certificate issued under the National Strategic Intelligence Act, 1994 (Act No 34 of 1994).

Accountability of Classification Review Panel

29. The Classification Review Panel is accountable to the National Assembly, and must report on its activities and the performance of its functions at least once a year.

Reporting

30. (1) The Classification Review Panel must, in respect of each financial year, prepare an annual report on the activities of the Classification Review Panel undertaken during the financial year.

(2) The Classification Review Panel must table the report contemplated in subsection (1) to Parliament within 30 days of receipt thereof if Parliament is in session, or if Parliament is not in session within 14 days after the commencement of the next Parliamentary session.

(3) The head of an organ of state must in respect of the declassified information in possession of that organ of state prepare a report for submission to the Classification Review Panel.

(4) The Classification Review Panel must on receipt of the reports contemplated in subsection (3) prepare a report on all the declassified information for the financial year in question and must include the report in its annual report referred to in subsection (1).

(5) The Classification Review Panel must, furnish any other report upon request by the Joint Standing Committee on Intelligence.

(6) The Chairperson of the Classification Review Panel must publish the annual report of the Classification Review Panel.

CHAPTER 8

APPEALS

Appeal procedure

31. (1) Any person who is refused access to information in terms of this Act may appeal to the relevant 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 therefore.

(3) Upon receipt of an appeal, the relevant Minister of an organ of state must make a finding and in the case of refusal provide reasons within 30 working days of the date of receipt of such request.

Application to Court

32. (1) A person who is aggrieved by a decision made with regard to a request for access to classified information may apply to a court for appropriate relief after the requester has exhausted the internal appeal procedure against a decision of the relevant Minister of the organ of state in question.

(2) Notwithstanding subsection (1) a requester may apply directly to a court for urgent relief contemplated in section 19 (3), without having exhausted the internal appeal procedure contemplated in section 31 of this Act.

CHAPTER 9

TRANSFER OF RECORDS TO NATIONAL ARCHIVES AND RELEASE OF DECLASSIFIED INFORMATION TO PUBLIC

Transfer of public records to National Archives

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

(2) Subject to section 17 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 must be declassified in accordance with section 14.

(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.

Release of declassified information to public

34. (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, 2000, and any other law.

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

(3) When an organ of state receives a request for records in its possession that contain state 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.

CHAPTER 10

IMPLEMENTATION AND MONITORING

Responsibilities of Agency

35. The Agency is responsible for monitoring —

(*a*) all organs of state for compliance with prescribed controls and measures to protect valuable information; and

(*b*) all organs of state referred to in section 3, excluding the South African Police Service and the South African National Defence Force for compliance with the prescribed control and measures to protect classified information.

CHAPTER 11

OFFENCES AND PENALTIES

Espionage offences

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

(a) to unlawfully and intentionally communicate, deliver or make available state information classified top secret which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state; or

(b) to unlawfully and intentionally make, obtain, collect, capture or copy a record containing state information classified top secret which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state.

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

(a) to unlawfully and intentionally communicate, deliver or make available state information classified secret which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state; or

(b) to unlawfully and intentionally make, obtain, collect, capture or copy a record containing state information classified secret which such a person knows or ought reasonably to have known will directly benefit a foreign state.

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

(a) to unlawfully and intentionally communicate, deliver or make available state information classified confidential which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state; or

(b) to unlawfully and intentionally make, obtain, collect, capture or copy a record containing state information classified confidential which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state.

(4) If a court is satisfied that substantial and compelling circumstances exist which justify the imposition of a lesser sentence than the sentence prescribed in this section, it shall enter those circumstances on the record of the proceedings and must thereupon impose such lesser sentence.

Receiving state information unlawfully

37. (1) It is an offence punishable on conviction by imprisonment for a period not exceeding 25 years to unlawfully and intentionally receive state information classified top secret which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state; or

(2) It is an offence punishable on conviction by imprisonment for a period not exceeding 15 years to unlawfully and intentionally receive state information classified secret which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state;

(3) It is an offence punishable on conviction by imprisonment for a period not exceeding five years to unlawfully and intentionally receive state information

classified confidential which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state.

Hostile activity offences

38. (1) It is an offence punishable on conviction by imprisonment for a period not exceeding 20 years for any person to —

(a) unlawfully and intentionally communicate, deliver or make available state information classified top secret which the person knows or ought reasonably to have known would directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic; or

(b) unlawfully and intentionally make, obtain, collect, capture or copy a record containing state information classified top secret which the person knows or ought reasonably to have known would directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic.

(2) It is an offence punishable on conviction by imprisonment for a period not exceeding 15 years for any person to —

(a) unlawfully and intentionally communicate, deliver or make available state information classified secret which the person knows or ought reasonably to have known would directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic; or

(b) unlawfully and intentionally make, obtain, collect, capture or copy a record containing state information classified secret which the person knows or ought reasonably to have known would directly or indirectly benefit a non state

actor engaged in hostile activity or prejudice the national security of the Republic .

(3) It is an offence punishable on conviction by imprisonment for a period not exceeding five years for any person to —

(a) unlawfully and intentionally communicate, deliver or make available state information classified confidential which the person knows or ought reasonably to have known would directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic; or

(b) unlawfully and intentionally make, obtain, collect, capture or copy a record containing state information classified confidential which the person knows or ought reasonably to have known would directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic.

Harbouring or concealing persons

39. 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 36 or 38 , is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 10 years.

Interception of or interference with classified information

40. (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 10 years.

(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 exceeding 10 years.

(3) Any person who unlawfully and intentionally 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 specifically 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 exceeding 10 years.

(4) Any person who_intentionally 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 exceeding 10 years.

(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 exceeding 10 years.

(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 programme 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 programme 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 programme 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 programme 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 programme 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 exceeding five years.

(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;

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

(iv) the offence was committed against a government facility of the Republic abroad, including an embassy or other diplomatic or consular premises or any other property of the Republic.

Registration of intelligence agents and related offences

41. (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 exceeding five years.

Attempt, conspiracy and inducing another person to commit offence

42. 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 information

43. Any person who intentionally and unlawfully discloses classified information in contravention of this Act is guilty of an offence and liable to a fine or imprisonment for a period not exceeding five years, except where such disclosure is -

(a) protected under the Protected Disclosures Act, 2000 (Act No. 26 of 2000) or section 159 of the Companies Act, 2008 (Act No. 71 of 2008); or

(b) authorised by any other law.

Failure to report possession of classified information

44. Any person who fails to comply with section 15 is guilty of an offence and liable to a fine or imprisonment for a period not exceeding five years

Provision of false information to national intelligence structure

45. 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 a fine or imprisonment for a period not exceeding five years.

Destruction or alteration of valuable information

46. Any person who intentionally and unlawfully destroys, removes, alters or erases valuable information is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding three years.

Improper Classification

47. Any person who intentionally classifies state information as:

(a) Top secret;

(b) secret; or

(c) confidential,

in order to achieve any purpose ulterior to this Act, including the classification of state information in order to—

(i) conceal breaches of the law;

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

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

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

(2)(a) In the event of subsection (1)(a) is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 15 years;

(b) in the event of subsection (1)(b) is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 10 years ;

(c) in the event of subsection (1)(c) is guilty of an offence and liable on conviction

to a fine or to imprisonment for a period not exceeding five years.

Failure by head of organ of state or official of organ of state to comply with Act

48. A head of an organ of state or an official of such organ of state who willfully or in a grossly negligent manner fails to comply with the provisions of this Act commits an offence and is liable on conviction to a fine, or to imprisonment for a period not exceeding two years.

Prohibition of disclosure of state security matter

49. 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) intentionally discloses such classified 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) intentionally publishes or uses such classified information in any manner or for any purpose which is prejudicial to the national security of the Republic;

(c) intentionally retains such classified 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 or fails to comply with any directions issued by lawful authority with regard to the return or disposal thereof; or

(d) neglects or fails to take proper care of such classified 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

exceeding 10 years, or, if it is proved that the publication of disclosure of such classified information took place for the purpose of its being disclosed to a foreign state to imprisonment for a period not exceeding 15 years.

Extra-territorial application of Act

50. Any act constituting an offence under this Act and which is committed outside the Republic by a citizen of the Republic or a person ordinarily resident 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

51. 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 STATE INFORMATION IN COURTS

Protection of state information before courts

52. (1) In any proceedings where an official or a functionary of an organ

of state intends to file a record that contains classified information, that official or functionary must alert court officials and the court of the classification of the information and request court officials to protect the record or parts of the record that contain classified information from disclosure or publication pending a court determination on the proper handling of such information during the course of the legal proceedings.

(2) Classified information that is filed in the manner contemplated in subsection (1) 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, orders full or limited disclosure, with or without conditions.

(3) 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 is not limited to—

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

(b) the protection from disclosure or 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 classified information.

(4) 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.

(5) If it appears to a court that it would, in any hearing held in terms of this section be in the interest of national security or in the interest of justice that

such hearing be held *in camera* or that the submission referred to in subsection (4) be not publicly disclosed, the court may direct that the hearing must be held *in camera* and that any person not authorised to receive such classified information may not be present at such hearing.

(6) 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 classified information in terms of subsection (2).

(7) A classification authority or the Director-General of the Agency, as the case may be, in consultation with the relevant Minister, must declassify state 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.

(8) 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.

(9) 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 five years.

(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 national security.

CHAPTER 13

GENERAL PROVISIONS

Reports

For the purpose of this section **" a head of an organ of state"** includes a head of a Service defined in section 1 of the Intelligence Services Oversight Act, 1994 (Act No. 40 of 1994).

53. (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 relevant Minister and forward a copy of such a 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 Classification Review Panel and 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 states.

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

Regulations

54. (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 countermeasures and contingency planning for the protection of state 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 state information is adequately protected, including the establishment of security committees and security policies within organs of state;

(e) procedure to be followed and manner in which valuable information must be protected from alteration, loss or destruction.

(f) the marking of classified documents;

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

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

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

(j) the reporting of security breaches at any organ of state: and

(k) the procedure to be followed and manner in which a record that is reported and returned under section 15 to the South African Police Service or Agency, as the case may be, must be dealt with.

(2) The Minister must make the regulations referred to in subsection (1) within reasonable period from the date on which this Act takes effect.

(3) The Minister, subject to the National Archives and Records Services of South Africa Act, 1996 (Act No. 43 of 1996), and after consultation with the Minister of Arts and Culture, may make regulations regarding the protection, transfer, destruction or alteration of valuable information and must publish the draft regulations for public comment.

(4) The Minister must, within 12 months of the commencement of this Act make regulations consistent with this Act regarding —

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

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

(c) national information security standards and procedures for the categorisation, classification, downgrading and declassification of state information, which standards and procedures include but are not limited to—.

(i) organisation and administration of state information security matters at organs of state;

(ii) personnel security, including training, awareness and security screening;

(iii) information and communication technology security;

(iv) physical security for the protection of state information in consultation with the Minister of Police; and

(v) continuity planning.

(5) Before the Minister makes regulations regarding any categories of state information in terms of subsection (4)*(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)*.

(6) Subsection (5) applies to any modification made to the categories of state information in terms of subsection (4).

(7) No regulation made under subsection (4), 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.

(8) Any draft regulations made under this section must be tabled in Parliament for approval at least 30 days before the regulations are promulgated.

(9) Any regulations made under subsection (1) may prescribe penalties of a fine or of imprisonment for a period not exceeding three years for any

contravention thereof or failure to comply therewith.

Transitional provisions

55. (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 54, or for a reasonable period from the date on which this Act takes effect, except—

(a) Chapter 3;

(b) section 15;

(c) section 34;

(d) section 19;

(e) Chapter 10;

(f) section 54;

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

(h) Chapter 13; and

(i) subsection (3).

(2) Subject to this Act any state information classified under the Protection of Information Act, 1982 (Act No. 42 of 1982), the MISS Guidelines or any other law must remain classified notwithstanding the repeal of such law.

(3) Subject to section 17 –

(a) Any state information classified under MISS Guidelines, the Protection of Information Act, 1982 (Act No. 42 of 1982) or any other law, must be reviewed and an audit report must be compiled by the head of the organ of state concerned on the classified status of all classified information held by that organ of state.

(b) The Agency must review and compile an audit report on the classified status of all classified information of a defunct organ of state or agency that has no successor in function.

(c) The relevant head of an organ of state or the Agency, as the case may be, must submit an audit report within a reasonable period to the Classification Review Panel.

(4) In conducting a review in terms of section 55 (2) the relevant head of the organ of state concerned or the Agency, as the case may be, must apply the conditions for classification and declassification in section 14 to

(a) confirm the classification of the classified information;

(b) declassify the classified information; or

(c) reclassify the classified information.

(5) The head of the organ of state concerned or the Agency, as the case may be, must in accordance with section 33 transfer the declassified information contemplated in subsection (3)(b) to the relevant archive.

Repeal of laws

56. (1) Subject to section 55, the Protection of Information

Act, 1982 (Act No. 84 of 1982), is hereby repealed.

Short title and commencement

57. This Act is called the Protection of State Information Act 2011 and comes into operation on a date fixed by the President by proclamation in the *Gazette*.