120906 adhoc

INCOMPLETE : ALL EVEN NUMBERED PAGES NOT COPIED !

REPUBLIC OF SOUTH AFRICA

Confidential: Working Document 5

ANC

As at 4 September 2012

PROTECTION OF STATE INFORMATION BILL

(As presented by Ad Hoc Committee on Protection of Information Bill (National Assembly)
(introduced as Protection of Information Bill [B6-2010])
(The English text is the official text of the Bill))

(MINISTER OF STATE SECURITY)

[B 6B—2010]

ISBN 978-1-77037-877-3

No. of copies printed 1 800

CHAPTER 3

POLICIES AND PROCEDURES

CHAPTER 4

STATE INFORMATION WHICH REQUIRES PROTECTION AGAINST ALTERATION, DESTRUCTION OR LOSS

CHAPTER 5

SYSTEM OF CLASSIFICATION, RECLASSIFICATION AND DECLASSIFICATION OF STATE INFORMATION

Part A

Classification

Part B

Declassification

CHAPTER 6

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

CHAPTER 7

CLASSIFICATION REVIEW PANEL

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 (Proclamation 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;

"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 in terms of 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 state 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,

"record" means recorded state information regardless of form or medium;
"regulations" means the regulations issued by the Minister in terms of this Act;
"relevant Minister" means any Cabinet member whose portfolio is affected by this Act;
"request for access" means a request for access contemplated in section 1 of the Promotion of Access to Information 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 state **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 the 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 **infringe on the constitutional rights of** the public or individuals **or deny them 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 **state** 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 a provision of another Act of Parliament ~~that regulates access to classified information.~~

(5) For the purposes of this Act a person has knowledge of a fact if-

(a) **the person has actual knowledge of that 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) he or she fails to obtain information to confirm the existence of that fact.

(6) 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.**

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

(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)~~ **The protection and classification of state information** 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;

(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; and

(j) in balancing the legitimate interests referred to in paragraphs *(a)* to *(i)* the relevant Minister, 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.

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

(3) 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 **members of Cabinet, Deputy Ministers and** certain individuals who carry a commensurate security clearance.

CHAPTER 3

POLICIES AND PROCEDURES

Policies and procedures

7. (1) The head of an organ of state, where applicable, must establish policies, directives and categories for classifying, downgrading and declassifying state information and protection against alteration, destruction or 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(4).

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 or 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

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 classified information must be declassified.

Nature of classified information

11. ~~**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 or 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

12. ~~**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 contained in section 14.

Classification levels

13. ~~**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 the 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 the 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 **irreparable or exceptionally grave harm** to the national security of the Republic.

Authority to classify state information

14. ~~**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 **or other provisions of this Act.**

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

(3) Only designated staff members may be given the authority to classify state information **as confidential**, 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 the 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

DELETE (6) to (9)

~~classified 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, **the Agency or the relevant classifying organ of state** ~~or the Agency~~ to be dealt with in the prescribed manner.

~~*Part B Declassification*~~

Authority to declassify classified 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 the 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 decision 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 for classification set out in sections 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

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

(3) **The National Assembly and the National Council of Provinces** 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. 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 **political** 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; and

(i) has been removed from an office of trust on account of misconduct involving theft, **corruption, maladmnistration** 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 National Assembly)~~ **Parliament** of a resolution calling for that member's removal as member from the Classification Review Panel.

(2) A resolution of the National Assembly and the National Council of Provinces-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 **National** Assembly **and the National Council of Provinces**.

(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)~~ **the Joint Standing Committee on Intelligence** for the removal of that person; and

(b) must remove a person from office upon adoption by ~~(the National Assembly)~~ **Parliament** 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.

CHAPTER 8

APPEALS

Appeal procedure

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

(2) Any appeal referred to in subsection (1) must be lodged within 30 days of receipt of the decision and the reasons therefore.

(3) Upon receipt of an appeal, the relevant Minister of the classifying 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 (Act No. 2 of 2000) ~~and~~ or 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

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 **that would** ~~(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 **that would** ~~*(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

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 and Possession of classified information

43. Any person who unlawfully and intentionally discloses classified **state** information in contravention of this Act is guilty of an offence and liable to a fine or imprisonment **as provided for in this Act**, except where such disclosure or **possession** —

(a) **is** 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)* is authorized by any other law~~

(b) is authorised by an internal mechanism as may be provided for by the Minister in regulations; or

(c) reveals criminal activity, including criminal activity for ulterior purposes listed in section 14 and 47 of this Act.

(ANC seeking guidance on 43 on cover of "internal procedure/s to be followed by members, former members, contractors, and their representatives including legal advisors, union officials, and co-employees for the purpose of disclosing wrongdoing")

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 unlawfully and intentionally 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~~ **two** years.

Improper classification

47. (1) 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 **Prevention and Combating of Corrupt Activities Act, 2004 (No. 12 of 2004) as well as any other** unlawful act or omission, incompetence, inefficiency or administrative error;

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

(iii) prevent embarrassment to a person, organisation or **the Agency** ~~(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; or

(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

(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 the 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 classified 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 the national security.

CHAPTER 13

GENERAL PROVISIONS

Reports

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.

(5) For the purpose of this section **"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).

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 counter- measures 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;

Transitional provisions

55. (1) The provisions of this Act are suspended from operation pending the establishment of 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), 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 the Agency ~~(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(3) 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 law

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*.

Chapter 5: Classification and declassification of state information

This chapter provides for—

- Nature of classified information;
- Method of classifying state information;
- Classification levels;
- Authority to classify state information;
- Conditions for classification and declassification;
- Report and return of classified records;
- Authority to declassify classified information; and
- Maximum protection periods.

Chapter 6: Regular reviews, request for access to classified information and status review

The head of an organ of state must review the classified status of all classified information held by that organ of state and must do so at any time but at least once every ten years. This chapter further provides for a request for access to classified information. In specific circumstances where the state information reveals evidence of a substantial contravention of, or failure to comply with the law or an imminent and serious public safety or environmental risk and the public interest in the disclosure of the state information clearly outweighs the harm that will arise from the disclosure, the head of the organ of state concerned must declassify the classified information in accordance with this Act.

Chapter 7: Classification Review Panel

This Chapter provides for the establishment of a Classification Review Panel that must review and oversee status reviews, classifications and declassifications, receive reports and receive once a year reviews on the status of classified information conducted by the organs of state.

Chapter 8: Appeals

This Chapter provides for an internal appeal procedure and an application to court procedure. In circumstances contemplated in section 19 (3) a requester may apply directly to a court for urgent relief.

Chapter 9: Transfer of records to National Archives and release of declassified information to public

This chapter provides for the transfer of classified information to the National Archives or other archives established by law. It further provides for the release of declassified information to the public in accordance with the provisions of this Act, the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) or any other law.

Chapter 10: Implementation and monitoring

This chapter provides for the responsibilities of the Agency.

Chapter 11: Offences and penalties

This chapter provides for the following offences: Espionage offences; receiving state information unlawfully; hostile activity offences; harbouring or concealing persons; interception of or interference with classified information; registration of intelligence agents and related offences; attempt, conspiracy, and inducing another person to commit offence; disclosure of classified information; failure to report possession of classified information; provision of false information to national intelligence structure; destruction or alteration of valuable information; improper classification; failure by head of organ of state or official of organ of state to comply with Act; prohibition of disclosure of a state security matter. The penalties may vary on the basis of the nature of the offence and the actual or potential harm