110729
adher note

(SLA re-draft)

[Directions] Conditions for classification

17. (1) For the purposes of classification, classification decisions must be guided by section 21 and the following:

(a) Secrecy **[exists]** is justifiable only when necessary to protect **[the]** national **[interest]** security;

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

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

(ii) restrict access to information in order to limit scrutiny and thereby avoid criticism;

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

(iv) unlawfully restrain or lessen competition; or

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

(c) the classification of information is an exceptional measure and should be conducted strictly in accordance with sections 11 and 15;

(d) information is classified only when there is—

(i) a clear, justifiable and legitimate need to do so; and

(ii) a demonstrable need to protect the information in the interest of national **[interests]** security;

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

(f) the decision to classify information must be based solely on the guidelines

and criteria set out in this Act, the policies and regulations made in terms of this statutory framework;

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

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

(i) classification decisions **[ought to]** must **[be assessed and weighed]** balance openness against **[the benefits of]** secrecy taking into account the following factors:

(i) The vulnerability of the information;

(ii) the threat of damage from its disclosure;

(iii) the risk of loss of the information;

(iv) the value of the information to the adversaries of the Republic;

(v) the cost of protecting the information; and

(vi) the public benefit to be derived from the release of the information;

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

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

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

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

(2) The application of the classification **[principles]** 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.

PROPOSED AMALGAMATION OF CLAUSES 17 AND 21

[Direction for classification]

Conditions for classification and declassification

[Directions] Conditions for classification and declassification

17. (1) **[For the purpose of classification, classification decisions must be guided by section 21 and the following:]** The decision to classify information must be based solely on the guidelines and criteria set out in this Act and the regulations.

[(1)] (2) **[For the purposes of classification, classification]** Classification decisions must be guided by the following:

(a) Secrecy **[exists]** is justifiable only when necessary to protect **[the]** national **[interest]** security;

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

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

(ii) restrict access to information in order to limit scrutiny and thereby avoid criticism;

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

(iv) unlawfully restrain or lessen competition; or

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

(c) the classification of information is an exceptional measure and should be conducted strictly in accordance with sections 11 and 15;

(d) information is classified only when there is—

(i) a clear, justifiable and legitimate need to do so; and

(ii) a demonstrable need to protect the information in the interest of

national **[interest]** security;

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

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

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

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

(i) classification decisions **[ought to]** must **[be assessed and weighed]** balance openness against **[the benefits of]** secrecy taking into account the following factors:

(i) The vulnerability of the information;

(ii) the threat of damage from its disclosure;

(iii) the risk of loss of the information;

(iv) the value of the information to the adversaries of the Republic;

(v) the cost of protecting the information; and

(vi) the public benefit to be derived from the release of the information;

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

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

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

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

[(2) The application of the classification [principles] 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.

Continued classification of information

21. (1) In taking a decision whether or not to continue the classification of information, the head of an organ of state must consider whether the declassification of classified information is likely or could reasonably be expected to cause [significant and] demonstrable harm to the national [interest] security of the Republic.

2] (3) Specific considerations with regard to the decision whether to classify 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 financial loss to a non-state institution or will cause substantial prejudice to such an institution in its relations with its clients, competitors, contractors and suppliers; or]**

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

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

[(2)] (4) The application of the classification [principles] 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 information must be declassified

Or

NEW CLAUSE

Declassification of information

XXX. When the conditions for classification contemplated in section 17 no longer exist, information must be declassified.

Report and return of classified records

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

Authority to declassify information

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

(2) The head of an organ of state is the declassification authority, but he or she may delegate authority to declassify and downgrade in writing to **[specified officials]** 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]** the Agency is responsible for the handling of classified records and the declassification of such records of a defunct organ of state or agency that has no successor in function.

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

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

Maximum protection periods

20. In accordance with section 11(2) of the National Archives of South Africa Act, 1996 (Act No. 43 of 1996) information may not remain classified for longer than a 20-year period unless the head of the organ of state that classified the

information, certifies to the satisfaction of his or her Minister, having regard to the criteria contained in Chapter 8, that the continued protection of the information from unlawful disclosure is—

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

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

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

CHAPTER 7

CRITERIA FOR CONTINUED CLASSIFICATION OF INFORMATION

Continued classification of information

21. (1) In taking a decision whether or not to continue the classification of information, the head of an organ of state must consider whether the declassification of classified information is likely or could reasonably be expected to cause **[significant and]** demonstrable harm to the national **[interest]** security of the Republic.

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

(a) expose the identity of a confidential source, or reveal information about the application of an intelligence or law enforcement investigative method, or reveal the identity of an intelligence or police source when the unlawful disclosure of that source would clearly and demonstrably damage the national

[interests] 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;

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

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

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

Regular reviews of classified information

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

possessed in that organ of state.

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

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

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

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

22 (1) [At least once every 10 years, the] The head of an organ of state must at least every 10 years review the classified status of all classified information held [or possessed in] by that organ of state.] The head of an organ of state may review the classified status of classified information at any time but must do so at least once every 10-years.

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

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

(4)] (2) When conducting a review, the head of an organ of state must apply the **[criteria]** conditions for the **[continued]** classification and declassification of information **[contemplated]** set out in this chapter.

[(5) Organs of state inform the Minister and the public of the results of the regular reviews]

[(5) Despite subsection (1), the head of an organ of state may review the classified status of classified information at any time.]

(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.

[(6)] (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 **[22(1) or (5)]** by that organ of state and submit such report to the Classification Review Panel for certification.

(b) **[The Minister]** 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 status review of classified information

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

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

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

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

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

(b) provide for the notification to the requester of the right to appeal a decision as provided for in section 25.

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

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

whenever the fact of its existence or nonexistence is itself classified as top secret].

CLAUSE 23 (as agreed)

23 (1) If a request is made for 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 information requested.

(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) The head of the organ of state concerned must declassify the classified information in accordance with section 19 and grant the request for information if that 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 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 section 23 (4) (a) on good cause shown

(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.

Status review procedure

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

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

CLASSIFICATION REVIEW PANEL

Establishment of Classification Review Panel

xx. (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 XXX in the performance of its, his or her functions.

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

Or

(b) Access to classified information may not be refused to the classification Review Panel on any ground

Functions of Classification Review Panel (agreed)

xx. (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) 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

xxx. (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) **[Other]** The other four members of the Classification Review Panel must be suitably qualified of whom at least one member—

(a) must have expertise in the Constitution and **[the]** law;

(b) must have knowledge and experience of national security matters; and

(c) 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 (as agreed)

xx. (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 (as agreed)

xx. (1) A member 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 xxx.

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

Remuneration of members and staff (as agreed)

xx. 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 (as agreed)

xx. (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

xx. (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) Where the Classification Review Panel sets aside or vary a classification decision taken by the head of an organ of state the Classification Review Panel may substitute its own decision for it.

(3)] (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.

[(2)] (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: (as agreed)

(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

Xxx 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 (as agreed)

xx. (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 **[submit]** 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 Classification Review Panel must, furnish any other report as the Joint Standing Committee on Intelligence, request.

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

Appeal procedure

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

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

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

CHAPTER 8

TRANSFER OF RECORDS TO NATIONAL ARCHIVES

Transfer of public records to National Archives

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

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

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

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

(b) abide by the reasonable directions of the originating organ of state.

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

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

(6) Where an organ of state fails to act in terms of part B of Chapter 6, classified records in possession of the National Archives or other archives are regarded as being automatically declassified at the expiry of the relevant protection

periods referred to in section 20.

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

CHAPTER 9

RELEASE OF DECLASSIFIED INFORMATION TO PUBLIC

Release of declassified information to public

27. (1) Classified information that is declassified may be made available to the public in accordance with this Act, the Promotion of Access to Information Act, 2000, and any other law.

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

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

(4) There is no automatic disclosure of declassified information to the public unless that information has been placed into the National Declassification Database as provided for in section 29.

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

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

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

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

(4) If the refusal to grant access to a classified record is taken on appeal in terms of the Promotion of Access to Information Act, 2000, the relevant appeal authority must consider the classification and may declassify such information.

Establishment of National Declassification Database

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

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

(3) The National Archives and Records Services of South Africa is

responsible for the management and maintenance of the National Declassification Database.

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

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

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

(7) No declassified information may be placed in the National Declassification Database, if access to such information may be refused in terms of the Promotion of Access to Information Act, 2000.

CHAPTER 10

IMPLEMENTATION AND MONITORING

Responsibilities of Agency

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

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

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

(c) provision of expert support and advice to—

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

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

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

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

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

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

(c) provision of expert support and advice to organs of state which require assistance in the—

(i) classification and declassification of information; and

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

(d) identification and exploration of best departmental practices;

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

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

streamlined programmes;

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

(h) supplying of annual reports to the Minister.

Dispute resolution

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

CHAPTER 11

OFFENCES AND PENALTIES

OFFENCES:
A head of an 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.

Espionage offences

For the purpose of this section "**the State**" means the Republic of South Africa.

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

(a) to unlawfully communicate, deliver or make available state information classified top secret which the person knows or ought reasonably to have known or suspected would :

(i) directly or indirectly benefit another state; or

(ii) would directly or indirectly prejudice the state; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing state information classified top secret which the person knows or ought reasonably to have known or suspected would:

(i) directly or indirectly benefit another state; or

(ii) would directly or indirectly prejudice the state.

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

(a) to unlawfully communicate, deliver or make available state information classified secret which the person knows or ought reasonably to have known or suspected would:

(i) directly or indirectly benefit another state; or

(ii) would directly or indirectly prejudice the state; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing state information classified secret which such a person knows or ought reasonably to have known or suspected **[will]** would :

(i) directly benefit another state; or

(ii) would directly or indirectly prejudice the state.

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

1(6)]—

(a) to unlawfully communicate, deliver or make available state information classified confidential which the person knows or ought reasonably to have known or suspected would :

(i) directly or indirectly benefit another state; or

(ii) would directly or indirectly prejudice the state; or

(b) to unlawfully make, obtain, collect, capture or copy a record containing state information classified confidential which the person knows or ought reasonably to have known or suspected would:

(i) directly or indirectly benefit another state; or

(ii) would directly or indirectly prejudice the state.

[Hostile activity offences

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

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

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

(2) It is an offence punishable on conviction by imprisonment

for a period not less than 10 years but not exceeding 15 years, [subject to section 1(6)]—

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

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

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

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

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

Harbouring or concealing persons

34. Any person who harbours or conceals a person whom he or she knows, or has reasonable grounds to believe or suspect, has committed, or is about

to commit, an offence contemplated in section 32 or 33, is guilty of an offence and liable on conviction to imprisonment for a period **[not less than five years but]** not exceeding 10 years **[, subject to section 1(6)]**.

Interception of or interference with classified information

35. (1) Subject to the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002), a person who intentionally accesses or intercepts any classified information without authority or permission to do so, is guilty of an offence and liable to imprisonment for a period **[not less than five years but]** not exceeding 10 years, [**subject to section 1(6)]**.

(2) Any person who intentionally and without authority to do so, interferes with classified information in a way which causes such information to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence and liable on conviction to imprisonment for a period **[not less than five years but]** not exceeding 10 years, **[subject to section 1(6)].**

(3) Any person who produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is 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 less than five years but]** not exceeding 10 years, **[subject to section 1(6]).**

(4) Any person who intentionally or knowingly utilises any device or

computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect state information, is guilty of an offence and liable on conviction to imprisonment for a period **[not less than five years but]** not exceeding 10 years, **[subject to section 1 (6)]**.

(5) Any person who contravenes any provision of this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users commits an offence and is liable on conviction to imprisonment for a period **[not less than five years but]** not exceeding 10 years, **[subject to section 1(6)]**.

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

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

"content of any computer" includes the physical components of any computer as well as any 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 less than three years but not exceeding five years, **[subject to section**

1(6)].

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

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

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

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

Registration of intelligence agents and related offences

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

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

(b) not employed or operating as an agent for a foreign intelligence or security service but is in the Republic with the expectation or potential of activation or re-activation as an agent of such an intelligence or security service,

must register with the Agency.

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

Attempt, conspiracy and inducing another person to commit offence

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

Disclosure of classified [and related] information

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

Any person who unlawfully discloses classified information in contravention of this Act is guilty of an offence and liable on conviction to imprisonment for a period **[not**

less than three years but] 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

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

Provision of false information to national intelligence structure

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

Destruction or alteration of valuable information

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

Improper Classification

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

(a) conceal breaches of the law;

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

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

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

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

Prohibition of disclosure of a state security matter

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

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

(b) publishes or uses such information in any manner or for any purpose which is

prejudicial to the security or interests of the State;

(c) retains such information when he or she has no right to retain it or when it is contrary to his or her duty to retain it, or neglects of fails to comply with any directions issued by lawful authority with regard to the return of disposal thereof; or

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

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

Extra-territorial application of Act

44. Any act constituting an offence under this Act and which is committed outside the Republic by any South African citizen or any person domiciled in the Republic must be regarded as having been committed in the Republic.

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

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