IFP COMMENTS ON "Working document 14"

Those highlighted in yellow and underlined or **bolded,** as the case may be, are amendment and those *highlighted in yellow and italicized* are comments proposed by the IFP, not IFP amendments, for we do not look at this Bill as a matter in which politics should play a role. Ideology perhaps, but not politics, as this is an institutional matter. Our ideological perspective is rooted in liberal democracy: we wish to avoid the ever present risk that one day the security tail may wag the majority-party dog, no matter who the majority party may be. For simplicity of presentation, we have not affected all consequential amendments. August 14, 2011

REPUBLIC OF SOUTH AFRICA

PROTECTION OF STATE INFORMATION BILL

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

(MINISTER OF STATE SECURITY)

[B6 —2010]

14 August 2011

BILL

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

PREAMBLE

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

ACKNOWLEDGING the harm of excessive secrecy;

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

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

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

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

CONTENTS

Section

CHAPTER 1
DEFINITIONS, OBJECTS AND APPLICATION OF ACT

Definitions and interpretation

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

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

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

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

"categories of information" means those groupings, types, classes, file series or integral file blocks of classified information that may be classified, designated declassified or downgraded together or in bulk;
"categorisation of information" means the process by which state information is placed into categories for purposes of classifying or designating such information and for purposes of declassification, downgrading and the lifting of the designated status of information;
"classification authority" means the entity or person authorised to classify state information and includes—
(a) a head of an organ of state; or
(b) any official to whom the authority to classify state information has been delegated in writing by a head of an organ of state;
"classification of information" means a process used to determine—
(a) the manner in which such information may be classified in terms of sections **[15 and 17]** 13 and 15; and
(b) the level of protection assigned to such information
(c) [**the level of protection assigned to certain information**
[(b) **the manner in which such information may be accessed and classified in terms of section 15;]**
"classified information" means **[the]** state information that has been **[determined]** classified under this Act**[, the Protection of Information Act, 1982 (Act No 42 of 1982), or the former Minimum Information Security Standards guidelines, MISS Guidelines or any other law to be information that may be afforded heightened protection against unlawful disclosure];**
"**Classification Review Panel**" means the Panel established under section **[xxx]** 22;
["commercial information" means commercial, business, financial or industrial information held by or in the possession of an organ of state;]
"confidential information" has the meaning assigned to it in section **[15]** 13(1);
"Constitution" means the Constitution of the Republic of South Africa, 1996;
"declassification authority' means the entity or person authorised under section **[19]** 17 to declassify classified information;
"declassification database" means the database which contains all declassified information considered by declassification authorities to be accessible by members of the public;
"declassification of information" means the authorised change in the status of information from classified information to unclassified information;
"department" means a department as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994);
"downgrading of information" means a change of **[classified and safeguarded]** classification of information from its existing level to a lower level **[status to be reclassified and safeguarded at a lower level];**
"file series" means file units or documents that are arranged according to a filing system or kept together because they—
(a) relate to a particular subject or function;
(b) result from the same activity, instruction, document or a specific kind of transaction;
(c) take a particular physical form; or
(d) have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use;
"foreign State" means any state other than the Republic of South Africa [**and includes any person acting or purporting to act for or on behalf of any faction, party, department, agency, bureau or military force of or within a foreign company, or for or on behalf of any government or any person purporting to act as a government within a foreign country.;]** *delete: it is absurd**!!***
"head of an organ of state" means—
(a) in the case of a department, the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994 (Proclamation No 103 of 1994), or the person who is acting as such;
(b) in the case of a municipality, the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998), or the person who is acting as such;
(c) in the case of any other institution, the chief executive officer or equivalent officer, of that public body or the person who is acting as such; or
(d) in the case of a national key point declared as such in terms of the National Key Points (Act No. 102 of 1980), the owner of the national key point;
"hostile activity" means —
(a) aggression against the Republic **[State]** ;
(b) sabotage or terrorism aimed at the people of the Republic **[State]** or a strategic asset of the Republic **[State]**, whether inside or outside the Republic **[State];**
(c) an activity aimed at changing the constitutional order of the Republic State by the use of force or violence; or
(d) a foreign **[or]** hostile intelligence operation [*each country collects intelligence on another: any type of security research may falls within the definition of intelligence without being hostile].*
"[identifiable damage" means significant and demonstrable harm];
"[information" means any facts, particulars or details of any kind, whether true or false, and contained in any form, whether material or not, including, but not limited to—

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

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

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

"**information peddling**" means the conduct referred to in section 40

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

(a) computer-based information systems, including software applications, computer hardware and data; and

(b) electronic and mobile communication systems and the transmission of data;

["information principles" mean the principles that guide the protection of information as set out in Chapter 2];

"information security" means the safeguarding or **[protecting]** protection of state information in whatever form **[and includes, but is not limited to—**

(a) **document security measures;**

(b) **physical security measures for the protection of information;**

(c) **information and communication technology security measures;**

(d) **personnel security measures;**

(e) **continuity planning;**

(f) **security screening;**

(g) **technical surveillance counter-measures;**

(h) **dealing with and reporting of information security breaches;**

(i) **investigations into information security breaches; and**

(j) **administration and organisation of the security function at organs of state to ensure that information is adequately protected];**

"integral file block" means a distinct component of a file series that must be maintained as a separate unit to ensure the integrity of the records and may include a set of records covering either a specific topic or a period of time;

"[intelligence" means any information, obtained by a national intelligence structure, for the purpose of crime prevention, investigation and combating or for the purpose of informing any government decision or policy-making process carried out in order to protect national security or to further the national [interest] security and includes the following—

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

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

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

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

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

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

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

"intelligence" means the process of gathering, evaluation, correlation and interpretation of security information, including activities related thereto; *what is "security information"??? Define!*

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

"Minister" means **[the President or]** the member of the Cabinet designated by the President in terms of section 209(2) of the Constitution to assume political responsibility for the control and direction of the intelligence services established in terms of section 209(1) of the Constitution;
"MISS Guidelines" means the Minimum Information Security Standards document as approved by Cabinet on 4 December 1996;
"National Archives" means the National Archives and Records Service of South Africa established by section 2 of the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996);
"national intelligence structures" means—
(a) the National Intelligence Coordinating Committee (Nicoc);
(b) the intelligence division of the National Defence Force;
(c) the intelligence division the South African Police Service; and
(d) the Agency;
["national interest of the Republic" has the meaning assigned to it in section 11;]
["national security" means the resolve of South Africans as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life and includes protection of the people and occupants of the Republic from hostile acts of foreign intervention, terrorist and related activities, espionage, and violence whether directed from, or committed within the Republic or not, and includes the carrying out of the Republic's responsibilities to any foreign country in relation to any of the matters referred to in this definition;]

(a) **"national security"** means the protection of the people of the Republic as a whole **[and]** or the territorial integrity of the Republic **[against]** from any present and clear threat of the following acts when such threat affects the Republic's stability, security, integrity or development:
(b) **[the threat of]** use of generalized force or generalized violence **[the use of force];**
(c) **[the following acts]**:
  (i) hostile foreign intervention,
  (ii) terrorism or terrorist and related activities,
  (iii) espionage
  (iv) information peddling,
  (v) **[exposure of State security matters]**[1],
  (vi) exposure of economic, scientific or technological secrets vital to the Republic's stability, security, integrity and development
  (vii) sabotage, and
  (viii) **[violence]**,
(d) whether directed from or committed within the Republic or not, and includes the carrying out of the Republic's responsibilities to any foreign country in relation to any of the matters referred to in this definition;

"[need-to-know" means a determination made by an authorised person that a person with a valid security clearance gains access to such classified information as may be necessary to enable him or her to perform his or her functions];
"non state actor" means any person or entity other than a state **[involved with]** engaged in a hostile activity";
"organ of state" means—
(a) any organ of state as defined in section 239 of the Constitution, including, but not limited to, any public entity as defined in section 1 of the Public Finance Management Act, 1999 (Act No. 1 of 1999) and section 3 of the Municipal Finance Management Act, 2003(Act No.56 of 2003);
(b) any facility or installation declared as a National Key Point in terms of the National Key Points Act, 1980 (Act No. 102 of 1980);
"original classification authority" means the **[head of the organ of state]** classification authority that authorised the original classification**[, or the person or entity authorised by the head of the organ of state to do so];**
"personal information" means any information concerning an identifiable natural person which, if disclosed, could reasonably be expected to endanger the life or physical safety **[or general welfare]** of an individual;
"[physical security" means the use of physical measures to—
(a) **prevent or deter unauthorised persons from accessing protected information;**
(b) **detect attempted or actual unauthorised access; and**
(c) **activate an appropriate response];**
"prescribed" means prescribed by regulation made in terms of section **[48]** 57;
"Promotion of Access to Information Act" means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
["protected information" means state information which requires protection against destruction, loss or unlawful disclosure];
["public interest" means all those matters that constitute the common good, well-being or general welfare and protection of the people of South Africa, the promotion of which, are required by, or are in accordance with the Constitution];

---

[1] If state security matters are covered by clauses 13 and 15, they are covered. If they are not, they should not be kept secret. Anything that matter can be classified and protected that way. Therefore, this criterion is to be deleted together with the related definition and clause.

"public record" means a record created or received by a governmental body in pursuance of its activities;
"record" means recorded information regardless of form or medium;
"regulations" [includes] means the regulations issued by the Minister in terms of this Act;
"request' means a request made by any person and in relation to –

(a) review means a request for a review of the status of classified information;
(b) access to classified information means the request submitted to the relevant head of an organ of state; or
(c) records means the request for the records of an organ of state;

"[requester" means any person who makes a request in terms of the provisions of this Act];
"**relevant Minister**" means any Cabinet member whose portfolio is affected by this Act;
"secret information" has the meaning assigned to it in section **[15]** 13 (2);
"security" means to be protected against danger, loss or harm and is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts;
"security clearance" means a certificate issued to a **[candidate]** person after the successful completion of a security screening investigation, specifying the level of classified information to which the **[candidate]** person may have access **[subject to the need to know]**;
"security committee" means the committee, comprising representatives from all the main functions or structures of an institution, charged with overseeing the development, implementation and maintenance of the institution's security policy;
"sensitive information" means information which must be protected from unlawful disclosure in order to prevent the national [**interest**] 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 operations" means any function, activity or process conducted by an organ of state which is authorised by law and is in accordance with the Constitution;
["state security matter" includes any matter which is dealt with by the Agency or which relates to the functions of the Agency or to the relationship existing between any person and the Agency;] *delete: if they are classifiable, this is redundant, if they are not, this makes 13 and 15 useless together with most of the Bill*
"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;
"[the state" means the state of the Republic of South Africa];
"this Act" includes regulations made in terms of section **[48]** 57;
"top secret information" has the meaning assigned to it in section **[15]** 13 (3);
["valuable information" means—

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

"valuable information" means information contemplated in this Act whose unlawful alteration, destruction or loss is likely to deny the public or individuals of a service or benefit to which they are entitled.

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

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

(Sub clauses 2 and 3 are FLAGGED)

[(4) For purposes of this Act a person is regarded as having knowledge of a fact if—
(a) **that person has actual knowledge of the fact; or**
(b) **the court is satisfied that—**
(i) the person believes that there is a reasonable possibility of the existence of that fact; and
(ii) the person has failed to obtain information to confirm the existence of that fact, and "knowing" shall be construed accordingly].

[(5) For the purpose of this Act a person ought reasonably to have known or suspected a fact if the conclusions that he or she ought to have reached are those which would have been reached by a reasonably diligent and vigilant person having both—
(a) **the general knowledge, skill, training and experience that may reasonably be expected of a person in his or her position; and**
(b) **the general knowledge, skill, training and experience that he or she in fact has.]**

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

Objects of Act

2. The objects of this Act are to—

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

Application of Act [2]

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

(2) The Minister, on good cause shown and on such terms and conditions as the Minister may determine, may by notice in the *Gazette*—
(a) exempt an organ of state or a group or class of organs of state from the application of the duty to establish departmental standards and procedures in terms of section 8;
(b) restrict or preclude an organ or state or a group or class of organs of state from exercising the authority to classify information in terms of Chapter 6;
(c) grant to an organ of state an extension of the 18 months period referred to in section 23(5);
(d) exempt an organ of state from declassifying information before such information is transferred to the National Archives or other archives in terms of section 26; or
(e) exempt an organ of state from section 30 (1) insofar as the section authorises the Agency to carry out on-site inspections and reviews for the purposes of monitoring the protection of information programs.

(3) The Minister, on his or her own accord or on a request made by an organ of state may, by notice in the *Gazette*—
(a) determine that an organ of state is to be regarded as part of another organ of state for purposes of this Act;
(b) determine that for purposes of this Act a part of an organ of state to be regarded as a separate organ of state as specified by the Minister;
(c) determine that a category of organs of state is for purposes of this Act to be regarded as one organ of state with such head of organ of state as the Minister specifies; and
(d) if there is doubt as to whether an organ of state is a separate organ of state or forms part of another organ of state, determine that for purposes of this Act the organ of state—
(i) is a separate organ of state; or
(ii) forms part of another organ of state.

CHAPTER 2
GENERAL PRINCIPLES OF STATE INFORMATION

State information

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

Protected information

[2] *Subject to the amendment of clause 7 and to the notion that everything not classified is accessible under PAIA, we have no great difficulties with this clause. One needs to avoid that organs of state develop their own criteria to classify information and reasons to withhold them under PAIA. Even the Natal Sharks Board will need to classify the location and combination of its safe and make the document contain such information not accessible under PAIA.*

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

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

General principles of state information

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

(a) Unless restricted by law **[or by justifiable]** that clearly sets out reasonable and objectively justified public or private considerations, state information should be available and accessible to all persons;

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

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

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

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

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

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

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

(i) measures taken in terms of this Act must—

(i) have regard to the freedom of expression, the right of access to information and the other rights and freedoms enshrined in the Bill of Rights; and

(ii) be consistent with article 19 of the International Covenant on Civil and Political Rights and have regard to South Africa's international obligations;

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

CHAPTER 3
NATIONAL INFORMATION SECURITY STANDARDS [AND DEPARTMENTAL] POLICIES AND PROCEDURES

National standards and procedures

7. (1) The Minister must, within 12 months of the commencement of this Act issue non-binding guidelines[3] to assist the persons or departments concerned, which guideline identify- —

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

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

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

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

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

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

(c) information and communication technology security;

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

(e) continuity planning.

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

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

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

(4) Subsection (2) applies to any modification to the categories of information **[prescribes]** identified in terms of subsection (1).

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

(6) Any person responsible for the classification of information shall apply this Act having had due regard to the guidelines contemplated in this section.

---

[3] *The Minister can place any such requirements in regulations. If referring to regulations, this entire section is redundant and all would be required is to make a succinct summary of what is dealt within this section and make it an additional suitable subject matter for regulations in terms of clause 57.*

[Departmental] Policies and procedures

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

(2) Each organ of state must establish **[departmental]** policies, directives and categories in terms of subsection (1) within **[18 months of the commencement of this Act]** six months of the date on which the regulations contemplated under section 7(1) are promulgated.

(3) **[Departmental]** Policies and directives must [**not be inconsistent with]** take into account the national information security standards [**prescribed in terms of]** referred to in section 7[4].

CHAPTER 4
INFORMATION WHICH REQUIRES PROTECTION AGAINST ALTERATION, DESTRUCTION OR LOSS

Process of determining information as valuable

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

(2) Items of valuable information and files, integral file blocks, file series or categories of valuable information must be entered into a **[departmental]** register of valuable information developed and maintained by an organ of state.

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

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

Protection of valuable information

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

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

(3) The destruction of public records is subject to the National Archives and Records Service of South Africa Act, 1996 (Act No.43 of 1996).

[CHAPTER 5
INFORMATION WHICH REQUIRES PROTECTION AGAINST DISCLOSURE
Part A
Sensitive Information

National interest of Republic

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

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

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

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

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

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

(3) Matters in the national interest include—

(a) **security from all forms of crime;**

(b) **protection against attacks or incursions on the Republic or acts of foreign interference;**

(c) **defence and security plans and operations;**

(d) **details of criminal investigations and police and law enforcement methods;**

(e) **significant political and economic relations with international organisations and foreign governments;**

(f) **economic, scientific or technological matters vital to the Republic's stability, security, integrity and development;**

(g) **all matters that are subject to mandatory protection in terms of sections 34 to 42 of the Promotion of Access to Information Act, 2000, whether in classified form or not.**

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

---

[4] *In terms of the Bill there must be the following levels of provisions (1) the Act, (2) the regulations in terms of clause 57, (3) the regulations in terms of clause 7, (4) written policies and (5) written guidelines. All such provisions must be consistent with each others, under pain of invalidity, that is if one can decide the criteria to resolve a conflict between provisions of (2) and (3)! In order to be valid an administrative action must be consistent with all such provisions and levels. The best way of getting out of this maze is to turn the regulations under (3) into the guidelines under (5) and do away with the statutory contemplation if (4). Every department can always develop policies without need for statutory enablement. Plus there are the Rules issued by the CRP.*

Part B
Commercial information

Nature of commercial information

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

(a) **Commercial information of an organ of state or information which has been given by an organisation, firm or individual to an organ of state or an official representing the state, on request or invitation or in terms of a statutory or regulatory provision, the disclosure of which would prejudice the commercial, business, financial or industrial interests of the organ of state, organisation or individual concerned;**

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

(2) Commercial information which may prejudice the commercial, business or industrial interests of an organisation or individual, if disclosed, includes:

(a) **commercial information that is not in the public domain, which if released publicly would cause financial loss, or competitive or reputational injury to the organisation or individual concerned;**

(b) **trade secrets, including all confidential processes, operations, styles of work, apparatus, and the identity, amount or source of income, profits, losses or expenditures of any person, firm, partnership, corporation or association.**

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

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

CHAPTER 6
CLASSIFICATION AND DECLASSIFICATION OF INFORMATION
Part A
Classification

Nature of classified information

[13] 11. Classified information—

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

(b) must be protected from unlawful disclosure and against alteration, destruction and loss as prescribed;**[when classified]**

(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 information in order to fulfil their official duties or contractual responsibilities; and

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

(e) must be classified in terms of section **[15]** 13 .

Method of classifying information

[14.] 12. (1) State information is classified by the relevant classification authority in terms of section **[17]** 15 when—

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

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

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

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

(3) The classification of information is determined through a consideration of the **[directions]** conditions as contained in section **[17]** 15**.**

Classification levels

[15.] 13. (1) State information may be classified as "Confidential" if the information is **[—(a)]**sensitive information, the **[unlawful]** disclosure of which is likely or could reasonably be expected to cause demonstrable harm **[may be harmful]** to the security or national [**interest**] security of the Republic or could reasonably be expected to prejudice the Republic in its international relations;

[(b) **[commercial information] the disclosure of which may cause financial clients, competitors, contractors and suppliers.]**

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

(a) sensitive information, the disclosure of which is likely or could reasonably be expected to cause **[serious]** grave[5] demonstrable harm to **[endanger]** the security or national [**interest**] security of the Republic or is likely or could reasonably be expected to jeopardise the international relations of the

[5] *By requiring harm to be "serious" in this section, by necessary implication the harm referred to in (1) needs not to be "serious" at all.*

Republic; or

[(b) **commercial information, the disclosure of which may cause serious financial loss to an entity;]**

[(c)] *(b)* personal information, the disclosure of which **[may]** is likely or could reasonably be expected to endanger the physical security of a person.

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

(a) sensitive information, the disclosure of which **[may]** is likely or could reasonably be expected to cause **[serious]** grave **[or]** and[6] irreparable harm to the national [**interest**] security of the Republic or **[may]** is likely or could reasonably be expected to cause other states to sever diplomatic relations with the Republic;

[(b) **commercial information, the disclosure of which may—**

(i) have disastrous results with regard to the future existence of an entity; or

(ii) cause serious and irreparable harm to the security or interests of the state;]

(c) personal information the disclosure of which **[may]** is likely or could reasonably be expected to endanger the life of the individual concerned.

(4) Subject to this Act The classifying authority must use the guidelines for classification levels as prescribed. *Where does this come from?? it was not in the Bill and I do not remember it having been agreed to! Without the qualification, given its positions, this can only mean that the "prescribed guidelines", (which is a contradiction in terms)can add additional criteria and grounds, which makes this provision not a ceiling but a floor!*

Authority to classify information

[16.] **14.** (1) Any head of an organ of state may classify or reclassify information using the classification levels set out in section **[15]** **13.**

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

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

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

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

(6) When state information is categorised as classified, all individual items of information that fall within a classified category are **[automatically regarded as]** deemed to be classified.

(7) Where a person is a member of Security Services as contemplated in chapter 11 of the Constitution who by the nature of his or her work deals with information that may fall within the ambit of this Act, that person must classify such information in accordance with the classification levels as set out in section **[13]** **11**.

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

(9) The information classified in terms of subsection (7) must remain classified until the head of an organ of state in question decides otherwise.

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

[[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**

---

[6] *See previous footnote. Plus, if an "or" is used rather than an "and" the first test will suffice, which would make the grounds for this classification identical to the preceding one, which is erroneous.*

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.]

[Directions] Conditions for classification and declassification

[17.] 15 (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]** conditions **[and criteria]** set out in this section **[this Act] [and the regulations].** *This was not in the erstwhile clause 17 which we instructed the law advisors to merely redraft without changing the agreed upon contents: there is a profound difference between "this Act" which includes its regulations and "this section".*

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

(2) *(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]** section **[15] 13**;

(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 relevant 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][7] *we would want this to stay in*;

(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]** but the information [**in question]** no longer

[7] To be discussed

requires high level classification, such information's classification **[and]** must **[should]** be downgraded.

(n) Information shall not be subjected to bulk classification or classification by category unless the applicable classification is warranted in respect of each piece of relevant information.

(2) When the conditions for classification contemplated in this section no longer exist, information must be declassified *This sub-clause is written below under clause 21, but it was agreed upon that it would be at the end of this section: otherwise which "section" does it refer to?*

[(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.] *We agreed that this comes out, as it is no longer necessary*

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

[Report and return of classified records

[18.] 16. 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, and knowing that such information is classified, must report such possession and return such record to a member of the South African Police Service or the Agency.] *We object to the State turning the citizen into a policeman or an intelligent officer: it is the State's job to look after and retrieve its secrets! If maintained the underlined insertion is necessary.*

Part B
Declassification

Authority to declassify information

[19.] 17. (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.] 18. 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[8] 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
(e) in compliance with sections 13 and 15

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.] 19. (1) **[At least once every 10 years, the]** The head of an organ of state-
(a) must at least every 10 years review the classified status of all classified information held **[or possessed in]** by that organ of state; or
(b) **[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.
(c) failing which it shall be deemed that said classification has lapsed[9]

[**(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

---

[8] *Chapter 8 does not provide for criteria*
[9] *If an organ of state cannot bother to put the "reviewed on __[date]__" chop on a document, file, or file cabinet or entire archive once every ten years, why should the constitutional values of openness, transparency and access to information suffer*?

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.] 20. [(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].

(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]** 17 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)] (iii) 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]** anticipate [*there is nothing to "condone" and no "non-observance": the issue was that of enabling the court to act before the deadline lapsed*, the time-period referred to in sub-section **[23]**(4)(a) on good cause shown where an urgent application is brought before court.

(6) If an application for a request referred to in subsection (1) is received, the head of the organ of state must within a reasonable time, to be no longer than 90 days of date of receipt of such a request, conduct a review of the classified information held by that organ of state relating to the request for declassification.

Status review procedure

[24.] 21. (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.

Proposal *whose?:*

(2) The head of an organ of state upon receipt of a request made in the prescribed manner for a review of the status of classified information must make a decision and in the case of refusal provide reasons within 90 days of date of receipt of such a request. *It seems to replicate 20(6): I have brought its contents there by amendment of that sub-clause*

Establishment of Classification Review Panel

[xx.] 22. (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]** 30 in the performance of its, his or her functions; and

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

Functions of Classification Review Panel

[xx.] 23. (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.

Add the functions set out for the Agency in terms of clause 38(1) which are functions of oversight, as these functions gel well the CRP's limited oversight functions contemplated in (1)(a) of this clause, and which, if left with the Agency, would make the Agency way too intruding in the functions of other organs of state, while districting it from its important core business at a possible great risk to national security!

[Constitution and] appointment of Classification Review Panel

[xxx.] 24. (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)] **[T]** 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]** the 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 **[at least one member]**—

(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

[xx.] 25. (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 un-rehabilitated 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

[xx.] 26. (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 National 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]** 25.

(5) A vacancy in the Classification Review panel must be filled as soon as practicable in accordance with section [**XXX**]. 24

Remuneration of members and staff

[xx.] 27. 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

[xx.] 28. (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]. 29. (1) The Classification Review Panel may confirm, vary or set aside any classification decision taken by the head of an organ of state and instruct the head of the organ of state concerned to change the classification status of the classified information, if necessary.

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

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

Appointment of staff

30. (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] 31. 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

[xx.] 32. (1) The Classification Review Panel must, in respect of each financial year, prepare an annual report on the activities of the Classification Review Panel undertaken during the financial year.

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

(3) The Classification Review Panel must, furnish any other report **[as]** upon request by the Joint Standing Committee on Intelligence **[, requests]**.

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

Appeal procedure

[25.] 33. (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, or fails to show satisfactory cause for a classification 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.] 34. (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]** 18 .

(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.] 35. (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) Subject to this Act, 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]** 37. *We wish to discuss this sub-clause: this could mean that until the NDB is established, which may not even happen on account of financial constraints, nothing can be released to the public. This also contradicts clause 18 and 34(2).*

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

[28.] 36 (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 and must do so if the relevant information requires mandatory disclosure in terms of Promotion of Access to Information Act.

(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.] 37 (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.] 38 **[(1) The Agency is responsible for ensuring implementation of protection of state 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] 33 ; and

(d) **making of recommendations to heads of organs of state and the Minister based on its findings]**; *This function would be better allocated to the CRP: see above*

(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.] 39. **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].** *It is unconstitutional to make this Minister a super Minister. A dispute across spheres of Government is regulated by chapter 3 of the Constitution and the legislation envisaged there. A dispute within a sphere of government is to be resolved constitutionally within the relevant cabinet or Exco.*

CHAPTER 11
OFFENCES AND PENALTIES

Offence to be inserted:

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.

CHAPTER 11
OFFENCES AND PENALTIES

Espionage offences

[32.] 40. (1) It is an offence punishable on conviction by imprisonment for a period not less than **[15]** 3 years but not exceeding **[25]** 15 years, **[subject to section 1(6)]**—

(a) to unlawfully and intentionally communicate, deliver or make available state information classified top secret which the person knows or ought reasonably to have known **[or suspected]** would directly or indirectly benefit a **[another]** foreign 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 benefit [another] foreign state.]** *This is absurd: it would create a crime of espionage even if no document is unlawfully disclosed and there is no intention to do so.*

(2) It is an offence punishable on conviction by imprisonment for a period not less than

[10] 2y ears but not exceeding **[15]**10[10] years, **[subject to section 1(6)]**—

(a) to unlawfully and intentionally 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 benefit a **[another]** foreign 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 benefit [another] foreign state.]** *This is absurd: it would create a crime of espionage even if no document is unlawfully disclosed and there is no intention to do so.* .

(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 and intentionally 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 benefit a **[another]** foreign 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 benefit [another] foreign state.]** *This is absurd: it would create a crime of espionage even if no document is unlawfully disclosed and there is no intention to do so.*

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

Receiving state information unlawfully

[Xxx] **41** (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)]** to unlawfully and intentionally receive state information classified top secret which the person knows or ought reasonably to have known **[or suspected]** would directly or indirectly benefit **[another]** foreign state; or

(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)** to unlawfully and intentionally receive state information classified secret which the person knows or ought reasonably to have known **[or suspected]** would directly or indirectly benefit **[another]** foreign state;

(3) It is an offence punishable on conviction by imprisonment for a period not less than three years but not exceeding five years, [**subject to section 1(6)**] to unlawfully and intentionally receive state information classified confidential which the person knows or ought reasonably to have known **[or suspected]** would directly or indirectly benefit [**another]** foreign state. *We wish the penalties in this clause to be adjusted to those we have proposed for espionage, but reduced by 1/3, for those who divulge are breaking a duty, while often those who receive are fulfilling a duty to their own country.*

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] 20 years, [subject to section 1(6)]—

(a) **[to] if a non state actor engaged in hostile activities unlawfully and intentionally communicate, deliver or make available state information classified top secret which [the person] that non state actor knows or ought reasonably to have known [or suspected] would directly or indirectly prejudice the [state] Republic; or**

(b) **[to] if a non state actor engaged in hostile activities unlawfully and intentionally unlawfully make, obtain, collect, capture or copy a record containing state information classified top secret which [the person] that non state actor knows or ought reasonably to have known [or suspected] would directly or indirectly prejudice the [state] Republic.**

(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] if a non state actor engaged in hostile activities unlawfully and intentionally communicate, deliver or make available state information classified secret which [the person] that non state actor knows or ought reasonably to have known [or suspected] would directly or indirectly prejudice the [state] Republic; or**

(b) **[to] if a non state actor engaged in hostile activities unlawfully make, obtain, collect, capture or copy a record containing state information classified secret which [the person] that non state actor knows or ought reasonably to have known [or suspected] would directly or indirectly prejudice the [state] Republic.**

(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] if a non state actor engaged in hostile activities unlawfully and intentionally communicate, deliver or make available state information classified confidential which [the person] that non state actor knows or ought reasonably to have known [or suspected] would directly or indirectly**

---

[10] *We have eliminated the possibility of these sentences to be mitigated by virtue of exonerating circumstances as per the old clause 1(6). In the United States the maximum sentence of these crimes, which applied during the cold war, is 10 years*!

prejudice the [state] Republic; or

(b) **[to] if a non state actor engaged in hostile activities unlawfully make, obtain, collect, capture or copy a record containing state information classified confidential which [the person] that non state actor knows or ought reasonably to have known [or suspected] would directly or indirectly prejudice [state] Republic .]**

42. (1) It is an offence punishable on conviction by imprisonment for a period **[not less than 15 years but]** not exceeding **[25]** [**20]** years **[subject to section 1(6)]** for a person to —

(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 benefit a non-state actor engaged in hostile activity [**or]** and [11]prejudice the **[state]** Republic; 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 benefit a non state actor engaged in hostile activity or prejudice the **[state]** Republic.

(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)]** for any person to —

(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 benefit a non state actor engaged in hostile activity [**or]** and prejudice the **[state]** Republic; 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 benefit a non state actor engaged in hostile activity or prejudice the **[state]** Republic .

(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):]** for any person to —

(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 benefit a non state actor engaged in hostile activity [**or]** and prejudice the **[state]** Republic; 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 benefit a non state actor engaged in hostile activity or prejudice the **[state]** Republic. *In respect of this clause, each sub-clause (b) is to be deleted for the same reasons stated in respect of espionage, and the penalties are to be reduced to the same level as espionage for the reasons stated in respect thereof*

Harbouring or concealing persons

[34.] **43** 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]** **40 or 42** , is guilty of an offence and liable on conviction to imprisonment for a period **[not less than five years but]** not exceeding **[10]** 5[12] years **[, subject to section 1(6)]**.

Interception of or interference with classified information

[35.] **44.** (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)].** *This seems on top of the other sanction as one*

---

[11] *Otherwise it makes no sense whatsoever. It would make "prejudice to the state" by itself sufficient to have" hostile activity", when in fact prejudice of the state is intrinsically occurring in any case of unlawful disclosure, as in terms of clauses 13 and 15 information can only be classified when prejudice to the state would occur if revealed. This offence would have the same description of unlawful disclosure. Plus, as written, this clause would apply to anyone, including journalists*

[12] *See comments set out under espionage. Plus he is a mere accessory after the fact,*

could not commit this offence without committing also one of the others.

(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 **[.]**; or

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

Registration of intelligence agents and related offences

[36.] 45 (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]**, *This would otherwise apply to any foreign policeman, soldier, or school guard, both in active duty or as reservist!*

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]** two years**, [subject to section 1(6)].**

Attempt, conspiracy and inducing another person to commit offence

[37.] 46 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 half the punishment to which a person convicted of actually committing that offence would be liable. *You can't punish ke who aids and abets on the basis of he who conceives and execute!*

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).]

47. 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.

Public Interest, Public domain and erroneous classification defenses

Xx (1) Anyone charged with an offence under this Act shall be entitled to raise as an exculpatory defence

(a) the improper classification of the information concerned, or

(b) the disclosure of the relevant information serving a reason of public interest or importance, which outweighs the reason for its classification.

(2) Any classified information which falls within the public domain or is disclosed in a manner which can make such information accessible by person other than those authorized to access it shall be deemed no longer classified or classifiable in terms of this Act, save in respect of anyone who first caused such information to become of public domain or so disclosed

Failure to report possession of classified information

[39.] 48 Any person who fails to comply with section **[18]** 16 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)]**. See comments in respect of clause 16

[Provision of false information to national intelligence structure] Information Peddling

[40.] 49 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. 50. **[Any person who unlawfully and intentionally 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].**

Any person who intentionally and unlawfully destroys, removes, alters or erases valuable information is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding three years [**or to both such fine and imprisonment].**[13]

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.]

51. Any person who knowingly classifies information as:

(a) top secret;

(b) secret; or

(c) confidential,

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

(i) conceal breaches of the law;

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

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

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

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

(c) in the event of subsection (1)(c) is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding five years.

[13] not required provided for in the Adjustment of Fines Act

Prohibition of disclosure of a state security matter

[43.] 52. **[(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)]. *Delete: If state security matters are covered by clauses 13 and 15, they are covered. If they are not, they should not be kept secret. Anything that matters can be classified and protected that way. Otherwise this makes 13 and 17 meaningless,*

[Extra-territorial] application of Act *It is a misnomer with which law professor ridicule legislators to their students!*

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

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

[45.] 54. 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, save in respect of section 51. *This clause enables the State to choose to protect its interest by not prosecuting offenders, but should not apply in respect of State officials in respect of offences which protect the public interest rather than the State interest.*

CHAPTER 12
PROTECTION OF INFORMATION IN COURTS

Protection of state information before courts
(clause flagged)

[46.] 55. (1) Classified information that is placed before a court may not be disclosed to persons not authorised to receive such information unless a court, in the interests of justice, and upon considering issues of national security**, [national [interest] security of the Republic]** as referred to in section 11 and any other law, orders full or limited disclosure, with or without conditions.

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

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

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

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

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

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

(5) A court may, if it considers it appropriate, seek the written or oral submissions of interested parties, persons and organisations but may not disclose the actual classified information to such persons or parties prior to its order to disclose the information in terms of subsection (1).

(6) A classification authority or the Director-General of the Agency, as the case may be, **[in consultation with the Minister]**, must declassify information required in legal proceedings, either in whole or in part, **[unless it is strictly necessary to maintain the classification in terms of this Act]**.*alternatively*, provided that any information capable of being used as a defence in criminal proceedings must be declassified. *Under no condition can the State convict the innocent man when the States withholds proof of his innocence.*

(7) In addition to the measures set out in this section, a court in criminal proceedings has the same powers as those conferred upon a court under section 154(1) and (4) of the Criminal Procedure Act,

1977 (Act No. 51 of 1977), and the said section applies with the necessary changes.

(8) Any person who discloses or publishes any classified information in contravention of an order or direction issued by a court in terms of this section is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 10 years.

(9) *(a)* The head of an organ of state may apply to a court for an order restricting the disclosure of unclassified state information that is part of, or is intended to be part of an open court record, which, if publicly disclosed or published, may undermine the national [**interest**] security.

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

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

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

CHAPTER 13
GENERAL PROVISIONS

Reports

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

[47.] **56.** (1) Each head of an organ of state must, by no later than 31 December of each year, submit a report to his or her Minister and forward a copy of such a report to the Minister and **[the Agency]** the Classification Review Panel 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 **[submits]** tables its report to Parliament, the Agency must forward copies of the report to every head of an organ of state.

Regulations

[48.] **57.** (1) The Minister may make regulations consistent with this Act regarding—

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

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

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

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

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

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

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

(g) the marking of classified documents;

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

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

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

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

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

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

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

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

(5) Any regulations made under subsection (1) may prescribe penalties of a fine or of imprisonment for a period not exceeding three years for any contravention thereof or failure to comply therewith.

Transitional provisions

[49.] 58. (1) The provisions of this Act are suspended from operation pending the establishment of the standards, policies and procedures contemplated in Chapter 3 and the regulations contemplated in section **[48]** 56, or for a reasonable period as determined by the President **[of 18 months]** from the date on which this Act takes effect**,[whichever occurs first,]** except—

(a) Chapter 3;

(b) section **[18,which provides for the reporting and return of classified records]** 16;

(c) section **[27 , which provides for the release of declassified information to the public]** 35**;**

(d) section **[28, which provides for requests for access to classified information in terms of the Promotion of Access to Information Act]** 36;

(e) section **[29, which provides for the establishment of the National Declassification Database]** 37;

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

(g) section **[48, which provides for the making of regulations]** 57;

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

(i) Chapter 13; and

(j) subsection **[(2)]** (3).

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

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

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

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

(3) Subject to section 20 –

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

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

(c) The relevant head of an organ of state or the Agency, as the case may be, must submit an audit report within a reasonable period[14] to the Classification Review Panel.

(4) In conducting a review in terms of section **[49]** 58 (2) the relevant head of the organ of state concerned or the Agency, as the case may be, must apply the conditions for classification and declassification in section **[17]** 15 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 **[26]** 34 transfer the declassified information contemplated in subsection (3)(b) to the relevant archive.

Repeal of laws

[50.] 59. (1) Subject to section **[49]** 58, the Protection of Information Act, 1982 (Act No. 84 of 1982), is hereby repealed.

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

Short title and commencement

[51.] 60. This Act is called the Protection of State Information Act, [2010] 2011, and comes into operation on a date fixed by the President by proclamation in the *Gazette*.

[14] Time period may be considered