MINISTRY
STATE SECURITY
REPUBLIC OF SOUTH AFRICA

PO Box 37, Menlyn, 0063, Tel: (012) 367 0700, Fax: (012) 367 0749
PO Box 51278, Waterfront, 8002, Tel: (021) 401 1800, Fax: (021) 461 4644

CLAUSE BY CLAUSE RESPONSE BY THE DEPARTMENT ON THE PROTECTION OF STATE INFORMATION BILL

INTRODUCTION

Herein follows the response of the Ministry of State Security on the proposed amendments to the Protection of State Information Bill made during the deliberations at the NCOP Ad Hoc Committee on the Protection of State Information Bill.

We will commence with the challenges we see in the proposed amendments beginning with the definitions and move on to deal with substantive clauses.

CHAPTER 1: DEFINITIONS, OBJECTS AND APPLICATION OF ACT

DEFINITIONS AND INTERPRETATION

In respect of the definitions appearing in Chapter 1, we are concerned with the proposed amendments from the parties. The reasons for this are contained here under.

Definition "Classified information" & "state information"

When the proposed amendments (ANC) on the above definitions are read together, they have a number of unintended consequences.

The proposed amendments include changing the term "classified information" to "classified state information". This means thatthe definition of classified state information would have to be read in conjunction with the definition of 'state information' and with the proposed amendments under the General Principles of state information,Clause 6 of the Bill,thatpropose that 'state information' may be protected against unlawful disclose, alteration, destruction or loss.

The consequences are that:

- The proposed amendments, in effect, enlarge the scope of protecting all state information, through non-disclosure, not just classified information and would hence increase the vetting responsibility of the state.
- Proposed amendments to valuable information extend the scope of valuable information to include more categories of

information than originally contemplated. This makes this category very wide and could mean any information that infringes on any constitutional right which makes it overbroad and not legally sound.

- Since valuable information is transactional informationthis would have the unintended consequence of restricting the ability of ordinary citizens in using "valuable information" to transact in their daily lives. The amendment is impossible to implement as it puts the onus on citizens to determine the lawfulness or otherwise of the disclosure of valuable information. This is more so when having to produce valuable information such as identity documents and passports to unknown persons.

- The intention of the Bill was to protect two types of information, **valuable information** and **sensitive information.** In respect to the former, the intention was to protect it from **unlawful alteration, destruction or loss** - so as to avoid the situation where the public is denied a service or benefit. The clubbing together of the different types of information is problematic because it brings valuable information within the realm of information protected from unlawful disclosure.The intention is not to regulate disclosure of valuable information as it is transactional. Sensitive information is information which must be protected from **unlawful disclosure** in order to protect our national security where it is in the public interest not to disclose such sensitive information.

Definition of "head of an organ of state"

Objections have been heard on the inclusion of municipalities under definitions of Head of Organ of State in (b). This was however derived from the definition of an organ of state in the Constitution. As defined in Section 239 of the Constitution, an organ of state is defined as any department of state or administration in the national, provincial or local sphere of government.

The motivation was to create synergy with the definition as in the Constitution.

Classification is not automatically extended to all organs of state. Organs can only classify documents after receiving authorization on good cause shown. It is important to point out that those organs of state that may opt-in would be subjected to the same rigorous procedures of classification as the security services and their classification would also be subject to Clause 12 and 14 and would only be allowed if they meet the criteria to protect national security.

However, information that relates to national security lies across organs of state. Hence wherever there is a need, the opt-in provision of the Bill would need to apply. A need may arise for a municipality to have the provisions of this Bill apply to it for example in instances of international cooperation agreements and obligations. In addition, we have established metropolitan police services that have policing powers to discharge their mandate,these include *inter alia* crime prevention, that may require the handling of classified information.

As such, the removal of (b) is a cause for concern. In the case of abuse, the provisions of Clause 14 prevail in respect of limiting when

information may be classified. A further safeguard in the Bill is the Review mechanism covered in Clause 18. The Bill carries severe sanctions in respect of wrongful classification by any person who intentionally classifies information in order to circumvent the criteria for classification set out in Clause 14.

Definition of National Security

The concept of "National Security" is governed by the following principles in Section 198 of the Constitution of the Republic of South Africa Act, 1996:

(a) National Security must reflect 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.

(b) The resolve to live in peace and harmony precludes any South African citizen from participating in armed conflict, nationally or internationally, except as provided for in terms of the Constitution or national legislation.

(c) National Security must be pursued in compliance with the law, including international law.

(d) National Security is subject to the authority of Parliament and the national executive.

We make the following submission for consideration:

- There is no universal or single definition of the concept of national security.
- This is mainly due to the fact that *what* the courts would consider suitable as a definition for national security would be dependent on the context, relevant circumstances and the specific needs for national security in each individual country.
- International jurisprudence reflects an inclusive approach to the definition of national security.
- The term is not specifically defined in the UK or European law due to the need to retain flexibility to ensure that a country may adapt to changing circumstances.
- The Canadians too do not have a clear definition of national security, but define "threats to the security of Canada" as having elements such as **espionage, sabotage, foreign influence activities, politically motivated violence, and subversion**. This is to avoid limiting the definition of national security.
- In the US, **they define national security broadly** and have identified the following elements as contributors to national Security namely, demographics, natural resources, the environment, economic growth, globalization, the quality of governance (national and international) technological developments, refugee crisis, peace-keeping, humanitarian emergencies and global health.
- It is important to note that the definition adopted by the National Assembly expressly excludes activities or freedoms

provided for in the Constitution, namely **lawful political activity, advocacy, protest or dissent.**

- The concept of national security is well recognised in South African Case law (cf Independent Newspapers v Minister of Intelligence Services 2008(5)SA31(CC)).
- The concept of **security** implies a threat to the integrity of the entity involved, be it of a person, a family, an organization and country.
- The definition needs to be aligned to the spirit of the Constitution and provide for all threats including new or emerging threats.
- The term "includes" therefore allows for emerging threats to the national security to be included. These threats are not static but dynamic. On the other hand, the term "means" would be restrictive to protecting the national security. The areas of priority are set by Cabinet following the presentation of the National Intelligence Estimate and overseen by the Joint Standing Committee on Intelligence.
- More importantly, "includes" in the definition National Security would be defined by the context when interpreted by the courts - therefore the word "includes" **cannot be read to mean that every instance can be included** under national security.

Clause (b)(i) within Definition of National Security

The deletion of this clause is a cause for concern for the following reasons:

- The clause on "hostile activities" is an important in the protection of national security as hostile acts refer to acts of "foreign intervention directed at undermining constitutional order".
- This definition recognises that there are non-state actors who pose a great threat relative to their size and resources.
- Hostile activity is also defined in the Bill to mean "aggression against the Republic, sabotage or terrorism aimed at the people or strategic asset of the Republic, an activity aimed at changing the constitutional order by the use of force.
- This definition encompasses activities of non-state actors.

Clause (b) (iii) within Definition of National Security

The deletion of this clause is a cause for concern for the following reasons:

- Espionage is not a new concept and is recognised in all countries. It is a serious national security issue in today's competitive world where foreign spies seek our strategic plans and knowledge of our capabilities and technologies to advance their interests at the expense of our own.

Clause (b) (v) within Definition of National Security

The deletion of this clause is a cause for concern for the following reasons:

- The Clause pertaining to exposure of economic, scientific or technological secrets vital to the Republic is not intended to bring back what was excluded initially under the term "commercial" information because the contents of this Clause relates to classified information vital to the republic and hence subject to the provisions of Clause 14 and 19.
- A nation that is economically insecure is subject to external influences and manipulation. Economic security today, arguably, plays a critical role in the attainment of national security. Today the global competitive nature of the world and the scramble for scarce resources manifests in foreign states employing interventions that counter the interests of other states. The US sanctions and their impact on our petrol prices is an example.
- The definition recognizes that in order to pursue the attainment of human and physical security for its people, the Republic has to engage in a number of policy choices and proactive strategies that would benefit the wellbeing of the economy and the people of the Republic. The focus on economic opportunities is an important aspect of intelligence work.

Definition of State Security Matter

The definition covers both classified and unclassified matters that fall under the ambit of the Agency and is therefore inclusive rather than narrowly defined.

However, it is proposed that:

- The definition is amended to include sensitive, valuable and tradecraft information.
- There is no need to change "includes" to "means" as it is contextual and will be interpreted in the context of the Agency's mandate in relation to national security.

THE INCLUSION OF VALUABLE INFORMATION IN THE BILL

The Deletion of valuable information in the Bill is a cause for concern because:

- The protection of valuable information is critical to the protection of human security which is the bedrock of national security. Further the failure to adequately protect valuable information could negatively impact on the sovereignty of the individual, State as well as the state's ability to protect the citizenry and residents.

- The Minister is responsible to protect critical information infrastructure as this is critical in securing the nation and sovereignty of the state. The protection of citizens' identity

ensures their fulfillment of all their aspirations such as in the cultural, economic and political spheres.

- The protection of valuable information is not adequately covered under other legislative dispensations as current legislation only criminalises wrongdoing such as the fraudulent alteration of information and hijacking of companies. This Bill, however, seeks to address the need to protect and criminalise the abuse of information. The objective is to create a conducive environment to secure the information and take preventive measures against the misuse of information.

CLAUSE 1(4): CONFLICT BETWEEN POSIB AND ANY OTHER ACT OF PARLIAMENT

Clause 1(4) speaks to how the Bill should be interpreted when a conflict arises between POSIB and any other Act of Parliament regulating access to classified information. Objections have been raised to the Bill taking precedence over PAIA.

It was submitted that the provisions of PAIA constitute the legislative articulation of the constitutionally protected right to access to information in Section 32 of the Constitution of the Republic of South Africa, 1996. It was hence argued that an attempt to render PAIA subordinate to the Bill in instances of a conflict between the provisions of PAIA and the Bill effectively renders the Constitution subordinate to the Bill. However, although PAIA gives effect to a constitutional right, it does not enjoy the same protection as the Constitution.

The POSIB and the PAIA have two different objectives in that PAIA was enacted to promote access to information whereas POSIB seeks to protect state information.

Protection of classified information to protect national security is mandated by the Constitution. The Constitutional Court in the matter of Independent Newspapers v Minister for Intelligence Services 2008 (5) SA 31 (CC) upheld the confidentiality claim to confidential state information premised on national security, and did do find the same to be constitutionally incongruent. It held that the protection of classified information to protect national security is mandated by the Constitution and necessary to protect the rights in the Bill of Rights.

This should not be confused with the role of the National Archivist to protect information in the National Archives of South Africa Act in relation to historical records.

Further, the POSIB provides that when requests are made for access to classified information under PAIA, the head of organ of state must consider whether to declassify the information in terms of Clause 19 of POSIB. If the information is declassified, then the Head of Organ of State must consider the granting of access to the information under the provisions of PAIA.

Clause 1(4) serves as a guide in interpretation in instances where another Act that regulates access to classified information is passed or where PAIA is amended in a manner that could conflict with the protections provided in POSIB. If you do not make express mention of PAIA in 1(4) then the court in a case of conflict of laws would have

no guidance as to how to interpret the legislation and which legislation takes precedence over the other.

PAIA does not afford sufficient protection for classified information:

- It does provide an information officer with the discretion whether to grant a request but falls short of providing guidance to the information officer on how that discretion should be exercised. Section 41 in PAIA provides that the information officer may refuse information where its disclosure could reasonably be expected to cause prejudice to the defence, security and international relations of Republic. The problem then arises that if the information that is requested falls outside the scope of Section 41 then the information must be disclosed in terms of Section 11, irrespective of its classification.
- PAIA itself recognises in section 5, that there may be other legislation that affects the disclosure of a record of a public or private body. There is therefore a need to ensure that in order to protect information that is classified, the POSIB will need to take precedence over PAIA but that this is a provision that applies only to classified information.
- PAIA does not provide a classification regime nor does it provide any mechanism for the protection of state information.

Legal opinion on the hierarchy of legislation in respect to POSIB and PAIA:

The Bill provides in Clause 1 (4) that it supersedes and takes precedence over the Promotion of Access to Information Act, 2 of 2000 ("the PAIA").

One of the consequences of this hierarchy is that requests for access to classified information shall to be dealt with in terms of the provisions in the Bill, and not in terms of the PAIA. The previous draft of the Bill provided that requests for classified information could be made in terms of the PAIA or the said Bill. Those provisions have been removed. Objection has been taken to this on the grounds that the Constitution requires that the PAIA should regulate requests for access to classified information.

The imbalance between the deferential standard for access to information in terms of the PAIA and the more exacting standard that was provided in the previous draft of the Bill for access to classified information meant that the potential conflict between the two would prove problematic.

The current Bill resolves the tension by making the Bill the dominant legislation.

The *Independent Newspapers* case (supra) upheld the confidentiality claim to confidential state information premised on national security, and did not find the same to be constitutionally incongruent. The Court held further that the protection of classified information to protect national security is mandated by the Constitution[1] and is necessary to protect the rights in the Bill of Rights.[2]

[1]See: Para 49
[2]See: Para 174

The protection of state information would therefore be competent and necessary in terms of the Constitution.

PAIA does not afford protection to classified information (save for information that falls in section 41 (2) of the PAIA, and then in terms of a more deferential standard for access), which could be obtained simply upon demand. This afforded no protection to such information notwithstanding the need for the protection of such information.

The objection is probably directed at the more exacting standard for access to classified information. In our view a more exacting standard for access to classified information would be justified, as was held in *Independent Newspapers*[3], even though this analysis was carried out in terms of the Court's inherent power to regulate its own process.[4]Clearly in determining where the appropriate balance lies the Court had to also consider the values in the Constitution[5].

In our view the separate provision in the Bill to request access to classified information does not render it constitutionally incongruent.

APPLICATION OF THE ACT

Clause 3(1)

The proposed amendment is a cause for concern. The extended definition of state information and its unintended consequences has

[3]See: Para 67
[4]See: Para 55
[5]See: Para 56

been dealt with, as has the issue of the inclusion of valuable information in the Bill.

Clause 3 (2) (a)

In respect to the proposal to delete the oversight structures from Clause 3(2)(a), this is a source for concern as these structures deal with classified information.

Clause 3 (2) (b)

In order to respond to submissions on the discretion of the Minister, an amendment is suggested that good cause shown be further clarified by setting out criteria that the Minister needs to consider in determining "good cause shown".

To this end, we propose that a new subsection be added.

Legal opinion on the power to extend the protection:

The Act is directed primarily at information held by the security services of the Republic and parliamentary committees that exercise oversight of security services.

The Bill provides in Clause 3 (2) (b) that its provisions may be made applicable to other organs of State. This will be regulated by regulations which will prescribe the manner in which application can be made for that to happen. The Minister may extend the Bill to other organs of State on good cause shown.

What constitutes good cause is not defined nor are any criteria laid down in the Bill for the exercise of the power.

A standard of good cause is not sufficient to provide objective criteria for the exercise of the power. The Act may be vulnerable to an attack on this basis. Consideration should be given to the considerations that must fall to be considered when exercising the power such as: the nature of the information handled by the organ of State, the access that is ordinarily available by members of the public to such information, the competence and ability of the officials in the organ of State to classify the information in accordance with the Bill etc.

If such criteria are not laid down, the potential exists for information that should be available under the PAIA, being subjected to secrecy in terms of the Bill, thereby infringing the right to access to information in terms of section 32 of the Constitution.

CHAPTER 2: GENERAL PRINCIPLES OF STATE INFORMATION

Proposals for Chapter 2 are a cause for concern for the following reasons:

The suggestions to move Clauses 4 & 5 to after the current Clause 6 would have the following impact:

- The inclusion of these Clauses under the General Principles diminishes the protection afforded to state information.
- This renders these clauses to be other principles.
- Whilst the intention may have been stylistic in the reorganization of the clauses, the clauses that have been moved under general principles are not general principles as

they do not speak to the norms and values which should be considered when interpreting the Bill.

- The clauses are being brought under the realm of normative value-based statements rather than the explicit statement of the protection that should be given to state information.
- By subsuming this Clause under the General Principles it confers a measure of discretion in the protection of state information.

It is proposed that the word "General" is removed from the heading of Chapter 2 to allow the flow of the sub-headings.

It was proposed that "some confidentiality and secrecy" in Clause 6(g) be replaced with "the protection of certain state information". This moves the debate away from established notions, from the notion of 'balancing secrecy with transparency' to the concept of the protection of state information. The principle of 'balancing transparency and secrecy' is established in the White Paper on Intelligence and is a product of consensus arrived at during national negotiations.

The White Paper on Intelligence further moots for a system of declassification, which should be considered to enhance the principle of public accountability and openness.

It was proposed that the words "may not be compromised" should be deleted from Clause 6(j) and replaced with "must be taken into consideration and may not outweigh all the legitimate interests that are referred to in paragraph (a) to (i)". The proposed amendment of this clause means that the other legitimate interests that are

referred to 6(a)-(i) cannot be protected, because they depend on national security being protected. National security is a prerequisite in a democracy for its continued existence and development.

CHAPTER 3 AND CHAPTER 4

The proposed amendments in these chapters are consequential amendments and hence have been dealt with in the previous chapters.

CHAPTER 5: CLASSIFICATION & DECLASSIFICATION

Clause 11 (a)

It was suggested that this clause should read: State information is classified by the relevant classification authority in terms of Section 14 when – "a classification authority has identified state information in terms of this Act as state information that **on careful consideration and sound legal grounds** warrants classification".

This would be redundant as any administrative official in exercising their functions must apply their minds and take decisions cognisant of the laws of the country – and if not, that decision can be overturned.

The Constitution directs that everyone has the right to administrative action that is lawful, reasonable and procedurally fair. Section 33 of the Constitution provided for national legislation to be enacted to give effect to this right and this was done through the promulgation

of the Promotion of Administrative Justice Act, No. 3 of 2000. This is part of the prerequisites of PAJA.

Classification levels:
Clause 12 (3)

In the clause that deals with Top Secret, it has been suggested to change "or" to "and" to amplify the heightened level of security. The amendment should be considered to distinguish between Secret and Top Secret doesn't distinguish the levels sufficiently.

To address this issue, we propose that for the level of Top Secret, the wording should be changed to read: "exceptionally grave harm". Opinion has been sought from the office of the State Law Advisor on this and they agree with this proposal to remove "serious or irreparable" and to replace it with "exceptionally grave".

Authority to Classify
Clause 13 (5) & 13(7)

The deletion of Clause 13(5) would render the system unworkable.

The issues raised in the proposed amendments to Clause 13(7) are to be dealt with in regulations.

Conditions for Classification and declassification
Clause 14

The proposal for this clause is here again consequential as these arise from amendments in other chapters and have been dealt with.

In respect of Clause 14 (2)(b)(1) the insertion of the word corruption has been considered but a well-established principle of interpretation of statutes provides that an express inclusion of one thing excludes the others. It is recommended that the Committee seeks the opinion of the office of Chief State Law Adviser on this proposal.

Clause 14(3) which proposes to replace "may" after the word "information" with the word "must" is a cause for concern.

However, the proposal to delete (d) (e) and (f) in this clause is a cause of concern as these are critical aspects of national security.
The proposal for a new Clause 14(6) is also a cause for concern as dealt with in our response to Clause 13(5).

Report and return of classified records
Clause 15

It was suggested that in Clause 15 the following is added: "or relevant classifying organ of state". The clause is agreed to.

The proposals to delete Clause 15 and replace it with wording that permits the non-return of classified documents is a cause for concern as this would work against the spirit of this Bill.

CHAPTER 6: REVIEWS, REQUEST FOR ACCESS, STATUS REVIEWS

Clause 19(3)(a)

We are concerned with the proposal to insert "or Clause 14" as this removes the discretion to grant or not grant a request for access once the classification is removed.

Clause 19(6)

In regard to a reasonable time, we submit that a court would be able to determine reasonable timeframes on a case by case basis. The 'notion of a reasonable time' as a timeframe recognises that it is problematic to determine a fixed period of time as this may not recognise the complexities of a specific review.

The proposal for a new clause 19(3) that refers to provisions of PAIAis supported but should be inserted as 19(7).

The further proposal to change 3(a)(i) with regard to the replacement of "substantial" with "any" as well as the change of the time frames is a cause for concern as these provisions are aligned to PAIA.

CHAPTER 7 CLASSIFICATION REVIEW PANEL

Establishment of the Classification Review Panel (CPR)

The recommendation to insert a new Clause 20(2) is a cause for concern as there is an already existing dispensation for the financing of independent structures.

Functions of the Classification Review Panel (CPR)

The proposed deletion of "with concurrence of the Minister" is a cause for concern because the Minister retains his executive functions in respect of the application of the Act.

In respect to Clause 22(2) to replace "National Assembly" to "Parliament", we will stand guided by the Committee.

Clause 23(h) is a cause for concern as this lowers the test for members to make it into the panel.

Clause 24 (2): The amendment is a cause for concern as the appointment of the panel forms part of regular appointments.

Clause 25: This is a cause for concern for the same reasons outlined in Clause 21(2)

Decisions of the Classification Review Panel (CPR)

Clause 27(1) and (2)

The proposed timeframes are a cause for concern because the **Classification Review Panel** in terms of Clause 21(2) must develop its rules for the proper performance of its functions including procedures regarding the deliberations and the conduct of the work. This is important; as this Bill did not intend members of the Classification Review Panel to be fulltime workers.

Clause 30 (3)

We suggest that rather than the proposed date of the 31st of December of each year that it would be more workable if the reporting period should be aligned with the financial reporting cycle of government.

Appeals procedure

Clause 31(1)

The proposal is a cause for concern as the functions of the panel are to deal with review and oversight and not appeals. To introduce an appeal function to the Panel would mean that they would review their own decisions which would be contrary to legal principle.

Clause 31(2)

In respect to the timeframe for appeals, the six month proposal has been noted but we are of the view that this should be aligned to PAIA and propose to change the 30 days to 60 days.

The independence of the Classification Review Panel:

The Panel is independent because its members are nominated by the general public then chosen by the Joint Standing Committee on Intelligence. The Joint Standing Committee is an oversight committee appointed in terms of Section 199 (8) of the Constitution, and is a multi-party Committee which acts as a safeguard against excesses in matters of security through its oversight to ensure transparency and accountability.

There is no reasonable foundation in the suspicion that this Committee will be partisan in any way in choosing persons who have in any event to be approved by the National Assembly. The fact that the National Assembly makes the final decision is a further safeguard that the members appointed to the Committee will be fit and proper persons. The process is a transparent one and public views about the candidates can be taken into account in the process.

The objection based on a perceived lack of 'independence' on the part of the Panel does not appear to have any reasonable basis. The public protector is seen as credible as a result of the same rigorous process and the activities whilst in office. To prejudge the Panel is not wise.

CHAPTER 11 Offences

Clause 35 (a)

The proposed amendment to this clause is a cause for concern – this is a consequential amendment from the deletion of valuable information.

Clauses 36, 37, 38, 39& 40

The phraseology "ought reasonably to have known" should be retained as there is no reversal of onus as has been submitted. The state would need to prove that the person ought to have known and would lead evidence in this regard. There is other legislation that refers to "ought reasonably to have known" and this phraseology was inserted at the recommendation of the NPA. Further Clause 51 of the Bill provides that no prosecution or preparatory examination in respect of any offence under the Bill which carries a penalty of imprisonment of 5 years or more may be instituted without the written authority of the National Director of Public Prosecutions.

With respect to replace "intentionally"with qualifying criteria we do not understand why the intention must be qualified. We believe the Bill provides sufficient means to declassify information. The Act of unlawful disclosure is punishable and there's no reason to make it more difficult to punish the act.

Proposals to reword Clause 39 which deals with Harbouring or concealing persons is a cause for concern as these deal with the serious offences of Espionage and Hostile Activity.

The qualification of intention is another cause for concern in Clause 40(6)(b)&(c).

Clause 36: Minimum sentences

The imposition of minimum sentences was a Cabinet decision.
Further the minimum sentences provide guidance to the courts and although the courts have discretion to impose lesser sentences in Clause 36(4), it is only where there are substantial and compelling circumstances that a lesser sentence may be imposed.

Further, the Constitutional Court upheld in **S v Dodo** that the minimum sentences provisions did not violate the principle of the separation of powers.

The courts have said that any legislation that results in sentences that are grossly disproportionate to the crime would be unconstitutional on the grounds that they would be cruel, inhumane and degrading.

The Criminal Law Amendment Act, 1997 allows for departures from the prescribed minimum sentences in "substantial and compelling circumstances", and has therefore been held to be a constitutionally mandated sentencing regime.

The Court in **S v Dodo** also felt that the "substantial and compelling circumstances" exemption, as interpreted by the Supreme Court of Appeal in **S v Malgas**, ensured that the courts were not required to impose a ***"grossly disproportionate" sentence*** that limits the right to dignity.

The periods of imprisonment are in line with international best practice and in most instances pose a lesser sentence than those imposed in other democracies.

The periods of imprisonment vary according to the nature of the contraventions and are intended to reflect the seriousness with which the respective contraventions are to be viewed.

Apart from the offence of espionage, none of the provisions that deal with the remaining categories prescribe a minimum sentence, only maximum sentences.

Legal opinion on sentencing:

There have been objections to the length of the sentences of imprisonment provided for in the Bill, and suggestions that these are disproportionate to the nature of the offence.

The Bill prescribes minimum and maximum sentences for various categories of espionage offences in Clause 36, based on the gravity of the offence, and treats the disclosure of top secret information to be more serious to the disclosure of secret information, and the disclosure of confidential information less serious to the disclosure of top secret and secret information.

In the case of espionage offences the Bill provides in Clause 36 (4) that the Court may impose a lesser sentence if there are substantial and compelling circumstances.

The Bill also creates other categories of offences such as receiving state information unlawfully (Clause 37), hostile activity offences (Clause 38), harbouring and concealing persons who contravene

Clauses 36 or 38 or who intend to do so etc. None of the provisions that deal with the remaining categories prescribe a minimum sentence, only a maximum sentence.

In our view the Bill does not violate the principle of separation of powers nor does it infringe the right not to be subjected to cruel and inhuman punishment.

Disclosure of classified information
Clause43

Clause 43 of the Bill makes it a criminal offence to disclose information, however, it provides for an exemption where:

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

(b) if a person who is charged for contravention of clause 43 is authorised by any other law to disclose classified information.

We disagree with the proposal that Clause 43 should be made to apply exclusively in respect of the terms of imprisonment in Clause 36. Due to the seriousness of the espionage offences in Clause 36 they attract higher penalties ranging from five (5) years in the case of "Confidential" information to twenty-five (25) years for "Top Secret" information.

Whistle blowers

Whistle blowers in the workplace enjoy protection under the provisions of the Protected Disclosures Act, No. 26 of 2000.

- In terms of this Act, members of the private and public sectors have a duty to act responsibly and in good faith in making disclosures for them to enjoy protection as provided in the PDA.
- In terms of the PDA, an employee is required to have reason to believe that information regarding any conduct of an employer or employee shows amongst others that:
  - a criminal offence has been committed or is being committed;
  - that a person has failed or is likely to fail or is failing to comply with a legal obligation; and
  - that the environment is being damaged or has been damaged.

The Bill makes it not a criminal offence to disclose in terms of the provision of the PDA arguing to the contrary is to miss the objectives of the clause. It is not to protect employees from what they were already protected from.

The inclusion of sub-paragraph (c) which refers to criminal activity is also rejected. As stated above, the Protected Disclosures Act lists extensive conditions for disclosures which includes the criminal nature of the impropriety that is the subject of the disclosure.

Secondly, where the information would reveal criminal activity there are adequate mechanisms for the Head of organ of State to review the classification (Clause 19(3)(a)(i)), review the decision of the Head of Organ of State by the Classification Review Panel (Clause 27(1));

appeal to the relevant Minister for access to the information (Clause31(1)); and apply to court with regard to any decision made above with regard to a request for access to classified information (Clause 32(1) and (2)).

The exclusion of Public Interest Defence clause

Various proposals to insert a public interest defence clause are a cause for concern. The reason for not including public interest has been reasoned and found to be risky. No other country provides for such as clause, except Canada, because of the following reasons:

- It is too risky to leave it up to the members of the public to decide what is in the public interest.
- The risk involved may entail that the public's decision may be wrong to believe that the disclosure is in the public interest.

In order to avoid that risk, drafters sought to include in Clause 19 a public interest override, instead of a public interest defence clause. The public interest override provides a mechanism to apply for access rather than to risk prosecution.

Clause 19 provides for the request for access to classified information and status review. This clause reads as follows:-

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

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

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

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

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

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

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

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

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

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

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

In terms of Clause 19 the head of the organ of state has no discretion, he must declassify information within 14 days of receipt of the request and grant the request for state information if there is evidence that reveals an imminent and serious public safety or environmental risk. Where there is evidence that reveals a substantial contravention of, or failure to comply with the law he must declassify information within 30 days of receipt of request and grant the request.

This is applicable where the public interest in the disclosure of the state information clearly outweighs the harm that will arise from the disclosure.
A court may condone non-observance of the time-periods referred to above on good cause shown where an urgent application is brought before it.

The approach adopted in Clause 19 ensures that any disclosure is done after the application has been granted and the information has been declassified.

If the public defence clause is included in the bill and the disclosure is done while relying on the defence clause, the risk accompanied by such disclosure is that the court will not accept that the disclosure was in the public interest in all circumstances. Where the court finds that the disclosure was not in the public interest, by then irreparable damage/harm would have been caused and the information so disclosed would already be in the public domain and impossible to retrieve.

The Canadian Legislation, the Security of Information Act, has been consulted in this respect:

- Section 15 (1) of the Security of Information Act ("the Act") provides as follows, "No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest".

- Section 13 reads as follows, "Every person permanently bound to secrecy commits an offence who, intentionally and without authority, communicates or confirms information that, if it were true, would be special operational information."

- Section 14 of the Act reads as follows, "Every person permanently bound to secrecy commits an offence who, intentionally and without authority, communicates or confirms special operational information".

- The defence applies to persons permanently bound to secrecy.

- Section 15 (3) of the Act deals with factors to be considered by the judge in determining whether a person acted in the public interest, which are as follows:-

> "that the person acted for the purpose of disclosing an offence under an act of Parliament and that he or she reasonably believed has been, is being or is about to be committed by another person in the purported performance of that person's duties and functions for, or on behalf of, the Government of Canada; and the public outweighs the public interest in non-disclosure."

- Prior to disclosure in terms of Section 15 (5) the judge or court may decide whether the public interest in the

disclosure outweighs the interest in non-disclosure only if the person has complied with the following:

"(a)the person has, before communicating or confirming the information, brought his or her concern to, and provided all relevant information in his or her possession to, his or her deputy head or, if not reasonably practical in the circumstances, the Deputy Attorney General of Canada; and

(b)the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to,

(i) the Security Intelligence Review Committee, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by another person in the purported performance of that person's duties and functions of service for, or on behalf of, the Government of Canada, other than a person who is a member of the Communications Security Establishment, and he or she has not received a response from the Security Intelligence Review Committee within a reasonable time, or

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported

> performance of that person's duties and functions of service for, or on behalf of, the Communication Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

It is clear therefore that according to this Canadian Legislation a person would not be found guilty of an offence if that person could establish that he or she acted in the public interest when communicating or confirming special operational information. The Act states that a person acts in the public interest if the person's purpose is to disclose "an offence under an Act of Parliament that he or she reasonably believes has been, is about to be committed by another person in the purported performance of that person's duties and functions for, or on behalf of, the Government of Canada." The public interest in disclosure of the information must outweigh the public interest in non-disclosure.

If an individual is charged with violating this part of the Security of Information Act, a judge or court can consider a public interest defence only if the individual followed a series of steps set out in the legislation before disclosing the special operational information as set out above.

The public interest definition contained in Section 15(1) is of limited application:

- It only applies to offence in terms of section 13 and 14 of the Canadian Act i.e. the intentional, unauthorised

communication of "special operational information" (confidential, military and intelligence-related information);

- It only applies with regard to persons who are "permanently bound to secrecy" (i.e. a current or former federal public servant or a person who has been specifically designated as permanently bound due to his access to special operational information and issues of national security); and it does not apply to more general statutory offences relating to the unauthorised communication, the unauthorised retention and the failure to take reasonable care of information sourced from the state, as well as the use of such information "in any manner prejudicial to the safety or interests of the state".

- The Canadian Access to Information Act, 1985 only makes provision for the public interest to override a classification if the information amounts to "third party information".

- The Canadian public interest defence clause therefore only applies to people permanently bound to secrecy after following a process of internal application similar to the process set out for "whistle-blowers" in the Protected Disclosures Act, 2000 after exhausting the internal mechanisms set out.

- The Canadian legislation provides that all persons are guilty of an offence if they have in their possession or control any secret official document or information.

We refer below to the legal opinion that has been obtained in respect to the Public Interest Defence and Public interest override.

Legal opinion on the public interest defence versus the Public interest override:

The Bill does not provide for what is described by various objectors as a public interest defence. The main concerns that underpin the objection are firstly that the absence of such a defence will have "a chilling effect on media freedom" and secondly this will discourage whistle blowers from disclosing wrong-doing within government in the public interest.

The argument premised on the protection of media freedom and for whistle blowers, are inter-related, as it is predicated on the notion of a disclosure of classified information without applying for the information to be declassified and provided legitimately through the machinery contemplated in the Bill.

An objection on this basis must also entail a consideration of the provisions in the Bill that cater for the process for declassification, the provision for access by the public to classified information and the checks and balances that ensure correct classification decisions. If the Bill makes adequate provision for these matters, it would have achieved the proper balance between the competing interests.

In other words the premise upon which the public interest defence rests is that the Bill is deficient in that notionally information that should not be classified, will be classified, and requests for access to such information will not be successful, necessitating a public interest defence for instances where classified information is disclosed in the public interest.

The Bill in Clause 14 prescribes strict conditions that must be satisfied for classification, which include *inter alia*:

(a) the overriding principle that information may only be classified when it is necessary to protect the national interest;

(b) information cannot be classified for improper purposes such as to conceal various kinds of wrong-doing or to avoid transparency;

(c) the information may only remain classified for as long as the protection is necessary;

(d) once the conditions for classification no longer exist the information must be declassified.

There is the additional safeguard that the Classification Review Panel, an independent oversight body, will carry out reviews to ensure the correct classification of state information.

It follows from these provisions that if information is classified to cover up wrong doing or to avoid disclosure when disclosure is otherwise in the public interest, then the information would fall to be declassified, and this ought to be uncovered by the Classification Review Panel and dealt with appropriately alternatively a request made in terms of Clause 19 for its disclosure, should be acceded to.

The refusal of access in terms of Clause 19 is subject to an appeal and may be reviewed by the Court, in terms of Clauses 31 and 32.

The Bill accordingly provides checks and balances to ensure there isn't an abuse of the authority to classify information, and provides for lawful means to gain access to the information. It does not countenance the principle of being an adjudicator in one's own cause, as is implied in the public interest defence.

The requirements of the Rule of Law, and the duty it imposes on all citizens including the media, are to respect classification decisions until they are set aside. To make special provision for the media and whistle blowers, would place them in a special category, which does not appear to be warranted, given the safeguards aforementioned and the provisions to request classified information.

It has been suggested that the Bill does away with the substantial protection afforded to whistle blowers in the Protected Disclosures Act, 26 of 2000 ("the PDA"), and the Companies Act, 71 of 2008.

As far as the PDA is concerned, it affords protection to a whistle blower from occupational detriment, and not from criminal sanctions. Nothing in the Bill dilutes the protection afforded to a whistle blower from occupational detriment. It therefore follows that the objection based on the contention that the protections afforded in the PDA are compromised, is without foundation.

Section 159 of the Companies Act deals with the protection of whistle blowers who disclose information that falls into any of the categories prescribed in section 159 (3) (b). None of those categories relate to classified information protected from disclosure in terms of the Bill. It accordingly follows that there is no merit in the contention that the Bill compromises the protection afforded in terms of section 159 of the Companies Act.

The Bill does, in any event, exclude from criminal sanction the disclosure of classified information in contravention of its provisions, where such disclosure is protected in terms of the PDA and section 159 of the Companies Act, or is authorised by any other law. This is dealt with in Clause 43 of the Bill.

In our view there does not appear to be a satisfactory constitutional argument for the provision of a public interest defence. None of the objectors have pointed to any democratic country where such a defence is recognised, and we have not been able to find one.

Clause 19 (3) (a) provides for a public interest override. The head of an organ of State must declassify the classified information and grant a request for access to the information if it reveals evidence of:

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

(b) an imminent and serious public safety or environment risk.

Clause 19 (3) (b) adds the further requirement that the public interest in the disclosure of the state information clearly outweighs the harm that will arise from the disclosure. The text in this Clause of the Bill needs to be improved to make the Clause grammatically correct, as sub-paragraph (b) is disjointed and needs to be linked to the preamble.

Public Domain Clause

On the matter of the Public Domain Clause, we submit the following opinion on the matter:

Legal opinion on the public domain clause:

Objection has been taken to the Bill for not excluding from the Clauses dealing with offences, the possession or disclosure of classified information once it was in the public domain.

The majority judgment in Independent Newspapers v Minister for Intelligence Services 2008 (5) SA 31 (CC) touched upon the issue as to whether once classified information was in the public domain it could remain secret and be prohibited from disclosure. It stated the following in [72]:

"Whether or not a document classified 'confidential' has been disclosed to some degree in the public domain is a relevant but not decisive factor in determining whether the document deserves continued protection. This is so because a leaked document does not lose its classification. If it were so, people may be encouraged to reap the benefit of their own misconduct by leaking classified or protected documents thereby rendering the documents beyond the protection they may deserve."

In the minority judgment of van der Westhuizen J, at [180], the learned Judge considered whether it would be rational to protect the secrecy of classified information once it was in the public domain, and stated the following:

"A court should take into account the availability of the information in the public domain, how the documents came to be in the public domain (illegal public disclosure will probably not bind the government in later litigation), and whether further disclosure would increase the risks of national security."

The type of issues raised in the above dicta fall within the criteria provided for in Clause 14 of the Bill. In other words there is no absolute protection of classified information once it is in the public domain, nor for that matter does it lose all protection once it is in the public domain. The continued protection of classified information in the public domain depends on whether the conditions for classification no longer exist, whether the protection is still necessary to protect national security, and whether the balance between

openness and secrecy may have shifted, to mention some of the relevant considerations in Clause 14.

If the conditions for classification no longer exist, then the possession and disclosure of the information cannot be penalised, as the information should not have remained classified at the point in time when that state of affairs came about.

If on a proper interpretation of the Bill it does not penalise the possession and disclosure of information that should not be classified, the objection then loses its force. In our view the Bill is not deficient as there is sufficient room to rely on a public domain defence by relying on the criteria in Clause 14 to show that the information should not have remained classified after it was available in the public domain. This would be an instance of a collateral challenge to the lawfulness of the decision to retain the classified status of the information.[6]

Improper classification
Clause 47

We are of the opinion that inserting "corruption or any unlawful act or omission", is repetition as it is adequately addressed in the preceding "breaches of law".

[6]See: Baxter, Administrative Law, 3d Impression (1996), pg 677; Oudekraal Estates (Pty) Ltd v City of Cape Town & Others 2004 (6) SA 222 (SCA) at [32]

Prohibition of disclosure of state security matter
Clause 49

Clause 49 prohibits the disclosure of information pertaining to a state security matter. Two options exist in this clause. One, the definition of the state security matter may be changed and restricted to valuable info, sensitive info and intelligence tradecraft, know-how, sources and methods. Or the clause may be deleted on condition that the legal opinion suggests that these matters are adequately protected in the SA legal dispensation.

A proposal will be made for this Clause following an opinion expected from the office of the State Law Advisor.

CHAPTER 12: PROTECTION OF STATE INFORMATION IN COURTS

The proposal for rewording of Clause 52 (6) is a cause for concern as it limits the courts from exercising its discretion.

CHAPTER 13: GENERAL PROVISIONS

The removal of valuable information has been dealt with previously.

Transitional Provisions

The proposal to amend Clause 55 is a cause for concern as it will remove the current protection afforded to previously classified information when the old law is repealed.

CLAUSE BY CLAUSE RESPONSE BY THE DEPARTMENT ON THE PROTECTION OF STATE INFORMATION BILL:

TECHNICAL AMENDMENTS TO THE BILL

1. Page 5: "categorisation of state information": line 14: replace the word **lifting** with the word **raising**.

2. Page 9: Section 7(1): line 16: add the word **reclassifying** after the word **classifying**.

3. Page 9: Section 7(3): line 22: replace the word **national** with the word **minimum**.

4. Page 9: Section 9(2): line 37: the words **must be made aware of the need** are vague and open to misinterpretation and abuse.

5. Page 10: Section 11(1)(c): line 23: who is to maintain the proposed register?

6. Page 13: Section 20(3)(b): lines 36 and 37: the clause is mangled and should read: **Access to classified information may not be denied to the Classification Review Panel on any ground**.

7. Page 13: Section 21(1)(a): line 40: insert the word **reclassifications** after the word **classifications**.

8. Page 13: Section 21(1)(b): line 43: insert the words **as per Section 53** before the last word **and**.

9. Page 13: Section 21(2)(a): line 50: insert the words **as per Section 53** before the semicolon.

10. Page 14: Section 22(3): line 8: the clause to read **with the support**, not **with a support**.

11. Page 17: Section 34(3): should we not attach a time limit to ensure that the process contemplated is completed within say three months?

12. Page 21: Section 49(d): line 39: the clause should read **the publication or disclosure**.

13. Page 23: Section 53(4): line 19: the last word should be **state** and not **states**.

14. Page 24: Section 54(4)(a) line 4: insert the word **reclassified** after the word **classified**.

15. Page 24: Section 54(4)(c): line 9: insert the word **reclassification** after the word **classification**.

16. Page 24: Section 54(9): line 33: the clause should read **penalties or a fine**.

17. Page 24: Section 55(3)(a): again the issue of a time limit.

18. Page 25: Section 55(3)(b) and (c): a time limit should be attached to (b), and in (c) the words **within a reasonable period** should be amended and made time specific.