Submission to the Ad-hoc Committee of the National Council of Provinces on the Protection of State Information Bill

Honourable Chairman and Members of the Ad-hoc Committee,

Introduction

The Right2Know Campaign (R2K) is a nation-wide coalition of people and organisations opposed to the Protection of State Information Bill in its current form. Our campaign is coordinated by working groups in the Western Cape, Gauteng, KwaZulu-Natal and more recently the Eastern Cape, as well as a national working group consisting of representatives from key civil society organisations, community groups and social movements across the country.
We believe that a responsive and accountable democracy able to meet the basic needs of our people is built on transparency and the free flow of information. Our founding statement—"Let the Truth be Known. Stop the Secrecy Bill!"—demanded that the Bill be drastically rewritten to bring it in line with the values of our Constitution and hard-won democracy.

Our vision

We seek a country and a world where we all have the right to know—that is to be free to access and to share information. This right is fundamental to any democracy that is open, accountable, participatory and responsive; able to deliver the social, economic and environmental justice we need. On this foundation a society and an international community can be built in which we all live free from want, in equality and in dignity.

About the Bill

Our founding statement identified seven key criteria—encapsulated in the R2K seven-point freedom test—as a minimum for legislation such as this to be consistent with the values of our Constitution and hard-won democracy.
We acknowledge the significant changes already brought about in deliberations of the National Assembly, which have resulted as much from people's struggles as from good sense on the part of political actors across the political spectrum, inside and outside Parliament, as well as on the part of the architects of the Bill.
However, there is some distance to go. This will be apparent from our analysis, below, of the shortcomings of the Bill when measured against the seven-point freedom test.
But before we emerge ourselves in the detail, here are some key issues to flag at the outset:

- The Bill burdens all of society with what should be a state problem, namely the keeping of state secrets. Ordinary people should not be criminalised for possessing and disclosing classified information—to do so will edge South Africa towards a "society of secrets", where free information exchanges and debate are inhibited by a culture of fear.
- The alternative means of protecting the public and a key demand of civil society, a public interest defence, remains absent from the Bill.
- The Bill's supposed remedies for public access, such as whistleblower protection and access to information/declassification procedures, remain seriously defective.
- The State Security Agency remains the beneficiary of unjustifiably heightened protection, not only for its work but its organisational being. This stretches the veil of secrecy beyond what is acceptable in a Constitutional democracy such as ours.
- The Minister and State Security Agency's role as "guardians" of other state departments' valuable information remains a problem.
- The Classification Review Panel is not independent enough and not accessible to ordinary people.
- Bad drafting in a number of instances has left the Bill in its current form wide open to abuse.

We thank the chairman and members of the Ad-hoc Committee for affording us their attention, and would appreciate an opportunity to engage further at the public hearings.

Murray Hunter, National Co-ordinator
on behalf of the Right2Know Campaign
February 17, 2012

www.r2k.org.za
t: 021 4617211
c: 072 672 5468

Measuring the Bill against R2K's seven-point freedom test

1.

Limit secrecy to core state bodies in the security sector such as the police, defence and intelligence agencies.

R2K believes that the power to classify information should reside with no more than the state bodies directly charged with national security matters, and that no obstacles should be placed on the free flow of information from and among other state bodies.

R2K welcomes the narrowing of the application of the Bill's classification provisions to core security bodies. However—

Concern 1.1—extension of application

The Bill provides:

> **3.** (1) …
> (2) The classification, reclassification and declassification provisions of this Act—
> *(a)* apply to the security services of the Republic and the oversight bodies referred to in Chapter 11 of the Constitution; and
> *(b)* may be made applicable by the Minister, on good cause shown, by publication in the *Gazette,* to any organ of state or part thereof that applies in the prescribed manner, to have those provisions apply to it.

R2K remains concerned at the apparent ease with which the Minister may extend the Bill's application to further state bodies. No parliamentary process and opportunity for public comment are provided.

Concern 1.2—Minister and SSA guard valuable info

The Bill provides:

> **35.** The Agency is responsible for monitoring—
> *(a)* all organs of state for compliance with prescribed controls and measures to protect valuable information; …

The Bill also empowers the Minister (in clause 54(1)) to make regulations regarding the protection of valuable information.
The Minister and SSA are not the appropriate bodies to prescribe and monitor other state organs' protection of valuable information. The Bill appears to assign them duties which are already assigned at least in part to the National Archives and Records Service. To advance government transparency, this task should not be left to a Minister and agency whose business is the keeping of secrets.
On a related note, the SSA's responsibility (in clause 16(4)) for the handling and potential declassification of records of defunct state bodies may cause some bias towards non-disclosure. It is not understood why this function is not given to a more neutral body.

2.

Limit secrecy to strictly defined national security matters and no more. Officials must give reasons for making information secret.

R2K believes that even the state bodies entrusted with the power to classify should exercise that power only to the extent it is—and they can show it to be—truly necessary to protect the security of the nation. The Bill must guard against undue and over-classification, and facilitate declassification to the greatest extent possible.

R2K welcomes the narrower definition (in clause 1(1)) of "national security". However—

Concern 2.1—exposure of state security matter

The Bill provides the following definitions:

> **1.** (1) In this Act, unless the context indicates otherwise— **…**
>
> **''national security''** includes the protection of the people of the Republic and the territorial integrity of the Republic against— …
> (iv) exposure of a state security matter with the intention of undermining the constitutional order of the Republic; …
>
> **''state security matter''** includes any matter, which has been classified in terms of this Act and, which is dealt with by the Agency or which relates to the functions of the Agency or to the relationship existing between any person and the Agency;

The protection afforded to "the exposure of a state security matter…" creates a circular reference when read with the definition of "state security matter".
As the definitions stand, it appears that any matter dealt with by, or relating to the functions of, the SSA may be considered per definition to be a national security matter and therefore classifiable.
The safeguard that there must be the "intention of undermining the constitutional order of the Republic" is no safeguard at all, as at the time of classification any intention of a person bent on exposing a state security matter would be purely hypothetical.
Put differently, on the current definition the SSA might consider itself justified to classify information about itself and its activities simply to prevent exposure, and not because the national security is at stake.
This may draw an unintended veil of secrecy over all aspects of the SSA's activities; even those that should properly be in the public domain to ensure accountability on the part of the SSA.

Concern 2.2—national security override

The Bill provides (in clause 6) laudable principles of state information, stressing inter alia the benefits of access to and free flows of state information. However, it also provides:

> **6.** …
> *(j)* in balancing the legitimate interests referred to in paragraphs *(a)–(i)* the relevant Minister, a relevant official or a court must have due regard to the security of the Republic, in that the national security of the Republic may not be compromised.

The peremptory language; "in that the national security of the Republic *may not be compromised* (our emphasis)", appears to defeat the purpose of instructing the decision maker to perform a balancing act. Rather, it appears to create a "national security override" inconsistent with Constitutional imperatives.

Concern 2.3—no reasons for classifying

While clauses 11 to 14 provide for the method of classifying state information, classification levels, authority to classify and conditions for classification and declassification, there is no provision that when information is classified, the responsible official must append reasons for the classification decision.
R2K believes that undue and over-classification will be curtailed should officials be required to apply their mind to the exact reason for the decision, at the time of the decision. It would also serve as an important safeguard for all interested parties, including the official concerned, should there be subsequent challenges to the appropriateness of classification decisions.

Concern 2.4—classification levels

The Bill provides for a distinction between "confidential", "secret" and "top secret" as follows (our emphasis):

> **12.** (1) State information may be classified as **confidential** if the information is sensitive information, the disclosure of which is likely or could reasonably be expected **to cause demonstrable harm** to national security of the Republic.
> (2) State information may be classified as **secret** if the information is sensitive information, the disclosure of which is likely or could reasonably be expected **to cause serious demonstrable harm** to national security of the Republic.
> (3) State information may be classified as **top secret** if the information is sensitive information, the disclosure of which is likely or could reasonably be expected **to demonstrably cause serious or irreparable harm** to the national security of the Republic.

It appears that there is no practical difference between the "cause serious demonstrable harm" required to classify as secret and the "demonstrably cause serious or irreparable harm" required to classify as top secret. This is so because of the use of the subjunctive ("or") rather than the conjunctive ("and") in subclause three.
On the current wording, information will be classified as "top secret" too readily.

Concern 2.5—authority to classify

The Bill allocates the authority to classify as follows:

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

> (2) A head of an organ of state may delegate in writing authority to classify state information to a staff member at a sufficiently senior level.
> (3) Only designated staff members may be given authority to classify state information as secret or top secret.
> (4) Classification decisions must be taken at a sufficiently senior level to ensure that only that state information which genuinely requires protection is classified.
> (5) …
> (6) Where a person is a member of the Security Services as contemplated in chapter 11 of the Constitution who by the nature of his or her work deals with state information that may fall within the ambit of this Act, that person must classify such information in accordance with the classification levels set out in section 12.
> (7) The member of the Security Services must submit the classified state information to the head of an organ of state in question for confirmation of the classification.
> (8) The state information classified in terms of subsection (6) must remain classified until the head of an organ of state in question decides otherwise.
> (9) The head of an organ of state retains accountability for any decisions taken in terms of a delegated authority contemplated in subsection (2).

Subclauses (1) to (4) attempt to ensure that classification decisions are taken at a sufficient level of seniority to reduce misclassification. However, it is problematic that the level of seniority is not defined.
But of even greater concern is subclauses (6) to (9), which provide that chapter 11 (police, defence and intelligence) officials may classify regardless of level of seniority, and that their classification decisions remain in force until and unless countermanded by their department heads. Since the Bill's application has been narrowed to those same state bodies (police, defence, intelligence), it means that the seniority safeguard is for all practical purposes no safeguard at all.

Concern 2.6—maximum protection periods

The Bill provides:

> **17.** In accordance with section 11(2) of the National Archives of South Africa Act, 1996 (Act No. 43 of 1996), information may not remain classified for longer than a 20 year period unless the head of the organ of state that classified the state information, certifies to the satisfaction of the Classification Review Panel that the conditions of classification set out in sections 12 and 14 still apply.

While the 20-year classification limit is welcomed, the exception to the rule is not—and the more so the apparent ease with which exceptions may be made. The words "certifies to the satisfaction of the Classification Review Panel" appear not to imply an explicit burden of proof.
In addition, there appears to be no requirement for further Classification Review Panel reviews of the classification status of such information. The cause of openness would be served should very regular reviews be required.

Concern 2.7—regular review reports

The Bill provides:

> **8…**

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

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

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

It is assumed that "must publish the annual report" on regular reviews means that the report must be made public. This is to be welcomed. However, the requirement that the report must be prepared "in the prescribed manner" (i.e. as per regulations) does not inspire confidence that sufficient information will be made public.
By way of example, at present the RICA judge's annual report on monitoring and interception as well as the Auditor-General's annual report on the intelligence services reveal information so minimal as to defeat whatever public confidence might have been instilled by the fact of public reporting.

Concern 2.8—transitional provisions

The Bill provides:

55…

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

(3) Subject to section 17—

(a) Any state information classified under MISS Guidelines, the Protection of 55 Information Act, 1982 (Act No. 42 of 1982) or any other law, must be reviewed and an audit report must be compiled by the head of the organ of state concerned on the classified status of all classified information held by that organ of state.

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

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

(4) In conducting a review in terms of section 55(3) the relevant head of the organ of state concerned or the Agency, as the case may be, must apply the conditions for classification and declassification in section 14 to—

(a) confirm the classification of the classified information;

(b) declassify the classified information; or

(c) reclassify the classified information.

Subclause (2) provides that all information previously classified—no matter that it occurred under the unconstitutional, apartheid-era 1982 Act or under the MISS Guidelines, which are of questionable legality—remains classified. Its unauthorised possession and disclosure will be subject to the same serious penalties as those reserved for unauthorised possession and disclosure of information properly classified under the new Bill.
Put differently, this transitional measure will have the effect, at least for the time being, of classifying vast swathes of information that would not be classifiable under the Bill—including information which was classified by state entities that now will not have the power to classify at all.
This measure is clearly not Constitutional.

It is not understood why, even if a prohibition on the *disclosure*, in the interim, of such information may be found to be justifiable, the prohibition on *possession*—as per clause 15 ("Report and return of classified records) and clause 44 ("Failure to report possession of classified information")—is not suspended pending the review prescribed in subclauses (3) and (4). At least, such a suspension will afford a proper opportunity to the many persons doubtlessly now in possession of classified information that should not be classified in the democratic era to apply for its declassification, without turning them into instant criminals.
As things stand, subclauses (3) and (4), which provide for the review of the classification status of information previously classified, provide the only potential succour—albeit too late for the numerous instant criminals.
But subclauses (3) and (4) suffer their own defects, including—

- They do not provide a time limit within which these reviews must take place (other than stating that reports must be submitted "within a reasonable period");
- They do not provide that the results of the reviews must be made public (i.a. so that members of the public may know the status of information they may have in their possession); and
- They do not grapple with the contradiction that the Bill itself will apply only to core security entities, while much of the information classified under the 1982 Act and MISS will have been classified by other organs of state too.

3.

Exclude commercial information from this Bill.

R2K believes that national security legislation such as this should not stray into the domain of commercial (or private) confidentiality. To the extent that such information may be worthy of protection, very different kinds of measures will do.

R2K welcomes the removal of provisions allowing for the classification of commercial and private information from the Bill. However—

Concern 3.1—commercial information

The Bill provides the following definition:

> **1.** (1) **…**
> **''national security''** includes the protection of the people of the Republic and the territorial integrity of the Republic against— …
> *(b)* the following acts: …
> (v) exposure of economic, scientific or technological secrets vital to the Republic;

The pertinent protection afforded to "economic, scientific or technological secrets vital to the Republic" may reopen the door to the classification of commercial information, which was previously excluded from the Bill.
The problem could have been ameliorated—but unfortunately is not—by the conditions for classification or declassification, which state:

> **14.** (1) …

(2) …
(h) scientific and research information not clearly related to national security may not be classified;

Thus, while there is a specific safeguard against the undue classification of "scientific and research information", there is no safeguard against the undue classification of economic information.

Concern 3.2—personal information

The Bill provides the following definition:

1. (1) …
'personal information'' means any information concerning an identifiable natural 60 person which, if disclosed, could reasonably be expected to endanger the life or physical safety of an individual;

It is not understood why the definition of personal information has not been deleted while the Bill does not regulate personal information.

4.

Do not exempt the intelligence agencies from public scrutiny.

R2K believes that even if the work of intelligence agencies may need to be protected from exposure where national security is at stake, this should be limited as far as possible—and the agencies themselves should remain transparent and accountable like any other democratic institution.

Concern 4.1—prohibition of disclosure of state security matter

This concern relates to the above "Concern 2.1—exposure of state security matter". There it was argued that the definition of "national security" in so far as it relates to "exposure of a state security matter", and when read with the definition of "state security matter", created a circular reference which will have the effect that any matter dealt with by, or relating to the functions of, the SSA may be considered per definition to be a national security matter and therefore classifiable.
This would draw a veil of secrecy not only over the secret activities of the SSA, but also over the SSA itself, severely limiting public accountability. In this regard we emphasise that a "state security matter" is defined not only as "a matter dealt with by", but also "relating to the functions of" the SSA. The veil of secrecy is stretched to the max.
Now, we draw attention to related problems introduced by clause 49, which provides:

49. Any person who has in his or her possession or under his or her control or at his or her disposal information which he or she knows or reasonably should know is a state security matter, and who—
(a) intentionally discloses such classified information to any person other than a person to whom he or she is authorised to disclose it or to whom it may lawfully be disclosed;

> *(b)* intentionally publishes or uses such classified information in any manner or for any purpose which is prejudicial to the national security of the Republic;
> *(c)* intentionally retains such classified information when he or she has no right to retain it or when it is contrary to his or her duty to retain it, or neglects or fails to comply with any directions issued by lawful authority with regard to the return or disposal thereof; or
> *(d)* neglects or fails to take proper care of such classified information, or so to conduct himself or herself as not to endanger the safety thereof, is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 10 years, or, if it is proved that the publication of disclosure of such classified information took place for the purpose of its being disclosed to a foreign state to imprisonment for a period not exceeding 15 years.

It appears that this clause was drafted to prevent SSA employees, contractors or sources from abusing their access to classified information. However, if that was the intention it is not the result—it clearly applies to "any person".
The result is that the general possession offence (clause 44 read with clause 15), the general disclosure offence (clause 43), the general hostile activity offences (clause 38), and the espionage offences (clause 36) are duplicated, with very problematic consequences:

- A two-tier offence system is created, giving protection to the SSA beyond that already given to all security agencies (police, defence force and SSA). This is so because clause 49 relates to "state security matters"—matters dealt with by or relating to the functions of the SSA.
- While the general disclosure offence (clause 43) is tempered by an exception where a disclosure is protected under the Protected Disclosures Act, clause 49 has no such exception. This gives the lie, in part, to the argument that the Bill in its current form gives whistleblower protection, as a prosecutor may circumvent a potential whistleblower defence by charging under clause 49, where no such defence is available, at least where SSA information is at stake.
- There is discordance between the penalties specified in clause 49 and the general offences. So, for example, the general possession and general disclosure offences (clauses 44 and 43) attract a fine or imprisonment of up to five years, while the same offences under clause 49 attract imprisonment of up to 10 years—no option of a fine.

The effect, we emphasise again, is to stretch the veil of secrecy over the work *and* the organisational being of the SSA far beyond limits acceptable in a Constitutional democracy.

5.

Do not apply penalties for unauthorised disclosure to society at large, only those responsible for keeping secrets.

R2K believes that the protection of state secrets is a matter that should concern the state and not be burdened on society as a whole. The state should protect its secrets at source and not criminalise ordinary people for exercising their Constitutional rights to access information and speak it freely when the state has failed its task.

During numerous public interactions on the Bill, proponents have claimed that a public interest defence, one of the key demands of R2K and others in civil society, "does not apply anywhere else in the world".
While it may be true that an explicit public interest defence is not included in legislation in many democracies, the argument ignores the reality that in those same countries members of the public are not prosecuted for the possession or disclosure of classified information (unless they are engaged in espionage, for example).
Thus, once Wikileaks had bolted the "Cablegate" horse, the US did not prosecute the websites, media organisations and millions of ordinary citizens who took possession of and proliferated the diplomatic cables. To do so, it was recognised, would constitute a breach of the First Amendment, which guarantees freedom of speech.
The only attempted prosecution thus far is that of Bradley Manning, the soldier who allegedly leaked the cables. And US authorities' investigation of Julian Assange of Wikileaks reportedly centres not on his possession and disclosure of the cables—which would be easy to prove—but rather on allegations that he had conspired actively with Manning; in other words that he was an accessory to Manning's alleged crime.
It must be acknowledged that the state may assume a slightly greater risk of the exposure of classified information when possession and disclosure by ordinary people is allowed. However, that risk is far outweighed by the intrusion of the Bill as it stands on ordinary people's rights of access to information and freedom of speech, and the values in general of our Constitution and hard-won democracy. The Bill will edge South Africa towards a "society of secrets", where fear of serious penalties will instill a culture of fear attached to free information exchanges and debate.
It must, however, be emphasised that exempting ordinary people from the possession and disclosure offences does not imply that they may not be prosecuted for espionage and hostile activity offences.

Concern 5.1—possession and disclosure criminalised

The Bill provides (our emphasis):

> **15. A person** who is in possession of a classified record knowing that such record has been unlawfully communicated, delivered or made available other than in the manner and for the purposes contemplated in this Act, except where such possession is for any purpose and in any manner authorised by law, must report such possession and return such record to a member of the South African Police Service or the Agency to be dealt with in the prescribed manner…
>
> **44. Any person** who fails to comply with section 15 is guilty of an offence and liable to a fine or imprisonment for a period not exceeding five years.

and:

> **43.** Any person who unlawfully and intentionally discloses classified information in contravention of this Act is guilty of an offence and liable to a fine or imprisonment for a period not exceeding five years, except where such disclosure is—
> *(a)* protected under the Protected Disclosures Act, 2000 (Act No. 26 of 2000) or section 159 of the Companies Act, 2008 (Act No. 71 of 2008); or 35
> *(b)* authorised by any other law.

and:

> **49. Any person** who has in his or her possession or under his or her control or at his or her disposal information which he or she knows or reasonably should know is a state security matter, and who—…
> … is guilty of an offence…

In each of these instances the offence should not apply to "a person" or "any person". With regards to possession and disclosure-related offences, the state should protect its classified information at source by imposing penalties on no more than persons with an original duty to protect the information, such as serving and former state employees, contractors and sources.

Concern 5.2—harsh penalties

Associated with our above concern that criminalisation of ordinary people will edge South Africa towards a "society of secrets", where a culture of fear will inhibits free information exchanges and debate, is the often very harsh penalties proposed in the Bill.
Without labouring the point, R2K questions whether the penalties specified for most or all of the offences are not drastically out of kilter with the values of our Constitution and hard-won democracy.

6.

Do not criminalise the legitimate disclosure of secrets in the public interest.

R2K believes that any protection of state information regime should allow "escape valves" to balance ordinary people's rights of access to information and freedom of expression with the state's national security mandate, in the interest of open and accountable democracy.

"Escape valves" appropriate to the values of our Constitution and hard-won democracy include:

- A public interest defence (the more so while the Bill criminalises the possession and disclosure of classified information by ordinary people);
- Appropriate whistleblower protection; and
- Appropriate access-to-information and declassification mechanisms.

R2K appreciates that some progress has been made towards the inclusion of the latter two, however—

Concern 6.1—no public interest defence

For as long as the Bill will expose ordinary members of the public to prosecution for the possession and disclosure of classified information, the only true remedy remains a public interest defence. The Bill contains nothing of the kind.
Proposals have been made by various civil society and media organisations regarding wording for such a defence. The proposals range from a defence mirroring the Promotion of Access to Information Act (PAIA) public interest override, to a simple balancing of the public's right to know against the putative harm of disclosure,

to a provision that the possession and disclosure of classified information that is wrongfully classified is not criminalised.
While R2K does not want to be prescriptive, clearly these proposals form a solid basis for a workable public interest defence.
This remains a key demand of R2K.

Concern 6.2—whistleblower defence: reversal of onus

The Bill provides:

> **43.** Any person who unlawfully and intentionally discloses classified information in contravention of this Act is guilty of an offence and liable to a fine or imprisonment for a period not exceeding five years, except where such disclosure is—
> *(a)* protected under the Protected Disclosures Act, 2000 (Act No. 26 of 2000) or section 159 of the Companies Act, 2008 (Act No. 71 of 2008); or 35
> *(b)* authorised by any other law.

R2K associates itself with the Open Democracy Advice Centre's submission in this regard, which points out: "Essentially, the protection for whistleblowers in section 43 makes the person accused of blowing the whistle on corruption or mismanagement bear the burden of proving that they blew the whistle."
Without duplicating the submission in its entirety, it bears repeating that since the Protected Disclosures Act (whistleblower) defence has been drafted as an exception, it will require the accused to prove that they qualify for that defence, rather than obligating the prosecution to prove that they committed the offence. This is not Constitutional.

Concern 6.3—whistleblower defence: can be circumvented

As the Bill stands the Protected Disclosures Act whistleblower defence can be invoked *only* should one be charged under clause 43, which is the general prohibition on the disclosure of state secrets. The defence may be unavailable to any person charged with unauthorised possession (clause 44 read with 15) or under the possession or disclosure provisions of information classified by the SSA (clause 49, the "Prohibition of disclosure of state security matter").
Thus, should a bona fide whistleblower disclose information classified by the police or defence force, he/she may be protected from consequences under clause 43. However, should the information have been classified by the SSA, a prosecutor could choose to pursue charges under clause 49, where the penalties are higher for the same actions and there is no whistleblower defence.
A similar circumvention is also available to prosecutors who may want to abuse the espionage offences clause (36) and hostile activity offences clause (38)—where for understandable reasons no whistleblower defence is included—to prosecute simple possession or disclosure. (Please refer to Concern 8.1 below, where we demonstrate how a drafting deficiency opens those offences to such abuse.)
From the above it should be clear that the whistleblower defence should not attach to clause 43 only, but should be available to bona fide whistleblowers under all circumstances.

Concern 6.4—access to information: PAIA overridden and duplicated

The Bill provides:

> **19.** (1) If a request is made for access to information and it is established that the information requested is classified, that request must be referred to the relevant head of the organ of state for a review of the classification status of the state information requested in terms of the provisions of this Act.
> (2) In conducting such a review the head of an organ of state must take into account the conditions for classification and declassification as set out in this chapter.
> (3) *(a)* The head of the organ of state concerned must declassify the classified information in accordance with section 14 and grant the request for state information if that state information reveals evidence of—
>
> (i) a substantial contravention of, or failure to comply with the law; or
> (ii) an imminent and serious public safety or environmental risk; and
>
> *(b)* the public interest in the disclosure of the state information clearly outweighs the harm that will arise from the disclosure.
> (4) The head of the organ of state must—
> *(a)* within 14 days of receipt of the request contemplated in subsection (3)(a)(ii) grant the request for the declassification of classified information; or
> *(b)* within 30 days, of receipt of the request contemplated in subsection (3)(a)(i) grant the request for the declassification of classified information.
> (5) A court may condone non-observance of the time-period referred to in 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.

"And" should be an or so that there is a lower threshold for public interest

and:

> **31.** (1) Any person who is refused access to information in terms of this Act may appeal to the relevant Minister of the organ of state in question.
> (2) Any appeal referred to in subsection (1) must be lodged within 30 days of receipt of the decision and reasons therefore.
> (3) Upon receipt of an appeal, the relevant Minister of an organ of state must make a finding and in the case of refusal provide reasons within 30 working days of the date of receipt of such request.

and:

> **32.** (1) A person who is aggrieved by a decision made with regard to a request for access to classified information may apply to a court for appropriate relief after the requester has exhausted the internal appeal procedure against a decision of the relevant Minister of the organ of state in question.
> (2) Notwithstanding subsection (1), a requester may apply directly to a court for urgent relief contemplated in section 19 (3), without having exhausted the internal appeal procedure contemplated in section 31 of this Act.

The above clauses establish a commendable attempt to provide a regime under which the public can access information that has been classified. However, as will be seen below it flounders in a number of respects.
It is not understood why the clauses above attempt to duplicate PAIA, which already has a well-established access *and protection* regime.
R2K associates itself with the submission made in this regard by the South African History Archive, save to say that the Bill's expedited procedure for access and appeal under certain exceptional circumstances as provided for in 19(3) should not be tossed out with the bathwater should it be decided to revert to PAIA itself as the mechanism for access.

The perception that under the Bill as it stands PAIA will still govern the general course of requests for access to classified information is unfortunately mistaken.
This is so because the Bill expressly overrides PAIA in clause 1(4), which states:

> 1…
> (4) In respect of classified information and despite section 5 of the Promotion of Access to Information Act, this Act prevails if there is a conflict between a provision of this Act and provision of another Act of Parliament that regulates access to classified information.

This being so, one is left with a commendably expedited access procedure when the exceptional circumstances under 19(3) apply—but no access procedure whatsoever when the exceptional circumstances do not apply. This effectively creates a new ground for refusal to provide access: the simple fact that a record has been classified. Again, R2K refers to the South African History Archive submission.
R2K believes that overriding PAIA—*the* key law in our Constitutional armature regulating access to information—is directly at odds with the values of our hard-won democracy, would tilt the scales well away from openness and accountability towards a security state, and should be scrapped.
The expedited access procedures in exceptional circumstances are commendable and worth retaining, but ideally should apply not only in respect of classified information, but all information. The question arises whether an amendment to PAIA is not the appropriate route.

Concern 6.5—access to information: public interest override defective

R2K joins the South African History Archive in pointing out a deficiency in the drafting of PAIA, which is replicated in the procedure for expedited application in exceptional circumstances.

PAIA provides (our emphasis):

> 46. Despite any other provision of this Chapter, the information oficer of a public body must grant a request for access … if—
> (a) the disclosure of the record would reveal 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 record clearly outweighs the harm contemplated in the provision in question.

The Bill provides (our emphasis):

> (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.

In both these instances, the conjunctive (“and”) determines that both conditions—i.e. “substantial contravention…” or ”imminent and serious … risk” *and* the public interest outweighing the harm need to apply. It appears that the intention of the legislature was, and international best practice is, for the “and” to be an “or”, which would strike

the correct balance so that where the public interest outweighs the putative harm, regardless of the circumstances, disclosure would be mandatory.

Concern 6.6—access to information: possession pending application

Another area where the Bill's attempt to give regulated access to information in the public interest may well fall down is in the contradiction between the prohibition on even temporary possession of classified information and the necessity to properly examine such information so as to prepare for an application for access, as well as to submit the classified record to an information officer, appeal authority or presiding officer in order to prove that the record contains the information one alleges should be disclosed.
Clauses 15 and 44 obligate any person who comes into possession of classified information to report and return such information to the police or SSA, on pain of a fine or jail sentence of up to five years.
Clause 15 provides:

> **15.** A person who is in possession of a classified record knowing that such record has been unlawfully communicated, delivered or made available other than in the manner and for the purposes contemplated in this Act, except where such possession is for any purpose and in any manner authorised by law, must report such possession and return such record to a member of the South African Police Service or the Agency to be dealt with in the prescribed manner.

While this clause does appear to allow retention "for any purpose and in any manner authorised by law"—and this may be interpreted as permitting retention pending an application for access—it would be far better to remove uncertainty by explicitly permitting retention—even qualified retention—pending an application for access.
Without such a provision, the access to information procedure provides a right which may more often than not be impossible to exercise.

Concern 6.7—Classification Review Panel not accessible to public

While once again commending the attempts, although imperfect, to provide access to information that has been classified, it should be pointed out that a right, for ordinary people, is often only as good as the money they can afford to ensure its realisation.
Thus, while media and other organised groups may afford the court appeals envisaged when access to information is denied, most ordinary South Africans will not.
To help remedy this, it has been suggested that the Classification Review Panel be empowered to consider appeals directly from the public, as an alternative to court. At present the Panel's functions (provided in clause 21) do not include any such power.

An independent body appointed by Parliament, and not the Minister of State Security, should be the arbiter of decisions about what may be made secret.

R2K believes that the Minister of State Security is not the appropriate authority to adjudicate classification and declassification decisions in other state departments as there is likely to be a bias in favour of secrecy.

R2K welcomes the proposed establishment of the Classification Review Panel. However—

Concern 7.1—Classification Review Panel not sufficiently independent

Chapter 7, which deals with the establishment, functions, constitution, membership, remuneration, meetings, decisions, staffing, accountability and reporting of the Classification Review Panel reveals a number of deficiencies tending to confirm a view that the Panel will be an extension of the SSA and not be sufficiently independent to remedy the original problem of the Minister as arbiter.

Clause 21 provides:

> **21…**
> (2) The Classification Review Panel may, with the concurrence of the Minister, make rules not in conflict with this Act for matters relating to the proper performance of the functions of the Classification Review Panel, including—
> *(a)* time periods within which reports by the heads of organs of state must be submitted;
> *(b)* state information to be supplied when a report is submitted;
> *(c)* procedures regarding the deliberations and the conduct of work of the Panel; and
> *(d)* random sampling methods to be employed in reviewing compliance under this Chapter.

The Minister's concurrence in the Panel's regulating function suggests a lack of independence.

Clause 22 provides:

> **22.** (1) Due regard having been given to—
> *(a)* participation by the public in the nomination process;
> *(b)* transparency and openness; and
> *(c)* the publication of a shortlist of candidates for appointment.
> (2) The Joint Standing Committee on Intelligence must table a list of five persons for approval by the National Assembly.
> (3) The National Assembly must by a resolution with a support of a majority vote of its members upon approval submit the list of five persons to the Minister for appointment….
> (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.

The Joint Standing Committee on Intelligence's being in charge of the nomination process may increase a bias towards secrecy among selected candidates for the Panel, and the Minister's appointment of the members suggests they will not be independent of him/her.
The renewability of the members' terms (though only for one term) suggests members would be more beholden to the Minister, who appoints them. Security of tenure for a single non-renewable term is likely to encourage independence.

Clause 24 provides:

> **24.** (1) A member of the Classification Review Panel may be removed from the Panel on—
> *(a)* the grounds of misconduct, incapacity or incompetence;
> *(b)* a finding to that effect by the Joint Standing Committee on Intelligence; and
> *(c)* the adoption by the Assembly of a resolution calling for that member's removal as member from the Classification Review Panel.
> (2) A resolution of the National Assembly concerning the removal of a member from the Classification Review Panel must be adopted with a supporting vote of a majority of the members of the Assembly.
> (3) The Minister—
> *(a)* may suspend a member from the Classification Review Panel at any time after the start of the proceedings of a committee of the National Assembly for the removal of that person; and
> *(b)* must remove a person from office upon adoption by the Assembly of the resolution calling for that person's removal…

Again, the Joint Standing Committee's being put in charge of procedures related to the removal of members, and the Minister's powers related to suspension and removal, suggest the Panel will be an extension of the state security architecture and not independent. A two-thirds majority in the National Assembly to endorse a removal decision, such as in the case of an independent institution like the Public Protector, may also be more appropriate.

Clause 25 provides:

> **25.** Members of the Classification Review Panel and staff of the Classification Review 10 Panel must be paid such remuneration and allowances as determined by the Minister with the concurrence of the Minister of Finance.

The Minister's power over remuneration is likely to increase a sense that the Panel is beholden to him/her.

8.

Additional concerns

We single out some additional concerns, although the list should not be regarded as exhaustive.

Concern 8.1—Espionage, Hostile Activity Offences open to abuse

Regarding espionage offences, the Bill provides:

> **36.** (1) It is an offence punishable on conviction by imprisonment for a period not less than 15 years but not exceeding 25 years—
> *(a)* to unlawfully and intentionally communicate, deliver or make available state information classified top secret which the person knows or ought reasonably to have known would directly or indirectly benefit a foreign state; or

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

Subclauses 36(2) and (3) mirror the above, albeit with lesser penalties in respect of lower levels of classification.

Regarding the receipt of state information unlawfully—essentially an extension of the espionage offences—the Bill provides:

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

Again, further subclauses mirror the same offence but with lesser penalties in respect of lower classification levels.

Regarding hostile activity offences, the Bill provides:

> **38.** (1) It is an offence punishable on conviction by imprisonment for a period not exceeding 20 years for any person to—
> *(a)* unlawfully and intentionally communicate, deliver or make available state information classified top secret which the person knows or ought reasonably to have known would directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic; or 20
> *(b)* unlawfully and intentionally make, obtain, collect, capture or copy a record containing state information classified top secret which the person knows or ought reasonably to have known would directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic.

Again, the same pertains regarding further subclauses.
It will be seen that in each of these provisions, the word “intentionally” has been inserted. This occurred late during the National Assembly Ad-hoc Committee process, in response to concerns that the provisions may be open to abuse. However, it appears that the insertion was done incorrectly, as in each case the word “intentionally” now attaches to the action (e.g. of communicating, delivering or receiving the classified information) rather than the purpose for which the action is taken (i.e. to “benefit a foreign state” or “prejudice the national security”).
As actions such as communicating, delivering or receiving are almost by definition intentional, the insertion of the word “intentionally” provide little succour. The intended legislative purpose will be achieved, however, if the intention is attached to the purpose, i.e. “with the intent to benefit a foreign state” or “with the intent to prejudice national security”.
To demonstrate the potential abuse on the current wording:

Example 1:

> An anti-corruption campaigner obtains classified records describing the acquisition of a major weapons system. The records reveal that no tender procedure was followed and twice the market value is being paid. The campaigner decides to risk the up to 5 years jail sentence for unauthorised disclosure as per clause 43, and publishes the documents on a website.
> However, an enterprising prosecutor decides to charge the campaigner not under 43, but with espionage. How? As per clause 36(1), the campaigner “knows or ought to

have known" that the disclosure "would directly or indirectly benefit a foreign state"—in this case because as a by-product of the disclosure, an enemy state got to know what type of weapons South Africa had acquired. While it certainly was not the intention of the campaigner to benefit the foreign state, he "should have known" and now faces 25 years in jail as a "spy" rather than a maximum of five as intended by the legislature.

Example 2:

An employee of the SAPS crime intelligence service comes across classified records in the course of her duties showing a top-secret operation against a major drug lord—but the same records show that the head of crime intelligence, who is supposed to be overseeing this operation, is in the drug lord's pocket.
After following the procedures prescribed in the Protected Disclosures Act, and believing herself to be covered by the whistleblower exemption in clause 43, she blows the whistle by handing the records to a member of parliament.
However, an enterprising prosecutor, realising the police officer is likely to claim whistleblower protection, decides to charge not under clause 43, but under the hostile activity offences (clause 38). How? As per the current wording of 38(1)(a), our SAPS officer "knows or ought reasonably to have known" that her actions would "directly or indirectly … prejudice the national security of the Republic".
Again, it was not the intention of the officer to prejudice national security—she had wanted to expose corruption—but she might have to admit that the by-product of her disclosure was that the drug lord got to know what was coming, and managed to evade arrest. In the event, she is unable to claim whistleblower protection, and is exposed to a 20-year jail term.

R2K believes unintended consequences and the abuse of the espionage and hostile activities offence clauses may be avoided by a simple redrafting to place the intention where it is due.

Concern 8.2—harbouring or concealing

The Bill provides (our emphasis):

39. Any person who harbours or conceals a person whom he or she knows, **or has reasonable grounds to believe or suspect**, has committed, or is about to commit, an offence contemplated in section 36 or 38, is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 10 years.

The inclusion of "reasonable grounds to believe or suspect" appears to be particularly harsh and harps back to apartheid-era law.

Concern 8.3—interception or interference

The Bill provides:

40…
(6)
(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.

It would appear that due to the way computer databases are organised and the way that search engines such as Google search them, it may well happen that innocent searches can, for example, land a person in restricted spaces on state computers, such as intranets or data lists, without the web surfer even being aware that he/she is intruding on restricted terrain. This is more likely to happen where the state computers are not protected by appropriate firewalls.
R2K is concerned that this provision, and others in clause 40, should be re-examined in light of the realities of modern web architecture.

Concern 8.4—protection of state information in courts

Clause 52 regulates the protection of classified information before the courts. R2K remains unconvinced that the principle of open justice and the court's discretion to regulate its own affairs are sufficiently taken into account.