P O Box 31719
Braamfontein 2017
South Africa
Tel: (011) 717 1941
Fax: (011) 717 1964
e-mail: foip@saha.org.za
www.saha.org.za
Physical address: William Cullen Library
University of Witwatersrand

PROTECTION OF STATE INFORMATION BILL

NCOP submission 17 February 2012

Introduction

The South African History Archive (SAHA) thanks the National Council of Provinces (NCOP) for the opportunity to comment on the Protection of State Information Bill (the Bill) currently being considered by the NCOP.

Established in 1988, SAHA is an independent human rights archive committed to documenting and promoting greater awareness of historical and, since 1994, contemporary struggles for justice. As well as servicing a traditional academic and research community (both domestically and internationally), the organisation positions notions of accessible archive and records as central components of the human rights and governance culture, discourse and practice. In this regard, SAHA promotes awareness, and tests the parameters, of South's Africa's access to information legislation, and ensures its archive is made available to communities and constituencies that ordinarily would not access these materials.

In 2001, SAHA established its Freedom of Information Programme (FOIP), and since then has been at the forefront of efforts to test the parameters of the Promotion of Access to Information Act (PAIA). Through FOIP, SAHA assists individuals, NGO's, activists and researchers with requests for information as well as submitting its own requests. In total SAHA has submitted over 1400 access to information requests to a range of public and private bodies. Since 2008, SAHA's FOIP has developed its work to become one of the lead organisations in South Africa offering training and capacity building to organisations and individuals who can most benefit from using PAIA.

With its considerable expertise, established reputation and distinctive commitment to ensuring all South Africans are aware of their right to access information, SAHA is well positioned to comment on the Bill.

SAHA acknowledges the improvements made to the Bill since its introduction in 2010. However, numerous problems remain with the Bill which, if enacted, will result in an unreasonable limitation on the constitutional right to information and unjust restrictions on the liberty of ordinary South Africans.

Classification of documents

Who can classify

Clause 3(2)(a) of the Bill restricts the right to classify information to "the security services of the Republic and the oversight bodies referred to in Chapter 11 of the Constitution".

However clause 3(2)(b) of the Bill allows the Minister to extend the power of classification to any organ of state. The definition of 'organ of state' includes any national, provincial or local department or administration and any body exercising a public power or performing a public function.

Furthermore, an 'organ of state' includes a facility or installation declared as a national key point in terms of the National Key Points Act 1980. That Act allows the Minister to declare any place or area as a national key point if the Minister considers it to be "so important that its loss, damage, disruption or immobilisation may prejudice the Republic, or whenever he considers it necessary or expedient for the safety of the Republic or in the public interest." OR Tambo airport is an example of a place that has been declared a national key point.

Under the Bill, the Minister is empowered to extend the right to classify information to such bodies without any process of consultation with the public or with the expert advisory panel (the Classification Review Panel) established under the Bill. There is no right for any party to appeal such a decision of the Minister.

The broad discretionary power afforded to the Minister has the potential to extend the operation of the classification provisions within the Bill beyond those public bodies that should properly be dealing with matters of national security. Accordingly clause 3(2)(b) should be deleted. In the event that a body not identified in clause 3(2)(a) of the Bill should require the power to classify documents, such permission should be sought via an amendment to the legislation which would involve the public consultation and parliamentary consideration and review that such an important amendment should be required to undergo.

What information may be classified

The test for classification

Clause 12 of the Bill authorises the classification of state information as confidential, secret or top secret based on the severity of the demonstrable harm to national security that may be caused by the disclosure of the information.

The test for what information may be classified as confidential, secret or top secret is presumably intended to be progressive, so that the higher the classification the higher the demonstrable harm that would result from the release of the information. However, currently the demonstrable harm required to classify information as top secret does not differ in substance from that required to classify information as secret.

In order to classify information as secret the disclosure of that information must be likely or reasonably expected to cause serious demonstrable harm to national security. The test for classifying a document as top secret is that the disclosure of the information be likely or reasonably expected to demonstrably cause serious *or* irreparable harm to national security (emphasis added).

Accordingly, the Bill would allow a document to be classified as either secret or top secret where its disclosure could be expected to cause serious demonstrable harm to national security. A document may also be classified as top secret where the harm caused would be irreparable.

Therefore the requirement to classify a document as top secret currently constitutes no higher threshold than the requirement to classify information as secret. The criteria for classifying information as top secret should be amended to be cumulative. That is, the test should be that the disclosure of the information would cause both serious *and* irreparable harm to national security.

The definition of national security and state security matter

In order to be classified under the Bill, information must relate to national security. The definition of national security is therefore central to the operation of the Bill. Unfortunately the definition currently contained in the Bill is unnecessarily broad and would allow the classification of information unrelated to national security.

The definition of national security is inclusive, rather than exhaustive. Therefore it would be possible for an organ of state to classify information they claimed would cause harm to national security that is not currently envisaged by the Bill. As broad categories of the type of information that may affect national security are provided in the Bill, it is unnecessary and unreasonable for further opportunity

for organs of state to identify information they consider relates to national security to be identified. Accordingly, the word 'includes' in the definition of national security should be replaced with 'means'.

Clause (b)(iv) of the definition of national security provides for protection against 'exposure of a state security matter with the intention of undermining the constitutional order of the Republic'. A 'state security matter' is also a non-exhaustive definition and includes any matter which has been classified under the Bill and is dealt with by the State Security Agency, or which relates to the functions of the agency or to the relationship existing between any person and the agency.

It is clear that the definition of a state security matter goes well beyond what could properly be considered to be a matter related to national security. For example, information about the relationship between any person and the State Security Agency would include all contracts between the agency and third parties. This would include cleaning contracts, contracts for the provision of drivers to officials and similar. Information about such contracts could not properly fall within any reasonable interpretation of national security.

Furthermore, any matter that could fall within the definition of a state security matter and properly be considered to relate to national security is already encompassed within other clauses contained in the definition of national security. Clause (b)(iv) of the definition of national security should therefore be deleted and all references to a state security matter in the bill, including the criminal sanctions in relation thereto (see clause 49 of the Bill), should be deleted.

Clause (b)(v) of the definition of national security provides for protection against 'exposure of economic, scientific or technological secrets vital to the Republic'. The inclusion of economic secrets in this provision renders the clause so broad as to extend the definition of national security well beyond what could fall within a reasonable interpretation of what constitutes national security.

For example, various mineral extraction operations may be vital to South Africa in terms of economic impact, such as maintaining a reasonable gross domestic product, managing the value of the rand and combating unemployment. However, none of these economic consequences are sufficiently related to national security to justify the inclusion of such matters in this Bill. The word 'economic' should therefore be removed from the clause.

Process of classification

Classification by category
The Bill does not require a determination regarding the conditions for classification to be undertaken in respect of individual documents. Rather clauses 7(1) and 13(5) authorise organs of state to make classification decisions in respect of broad categories of information. On making such a determination, any information that falls within that category will automatically be considered classified.

While SAHA acknowledges that the classification of individual documents would be more resource-intensive than classifying documents according to categories, SAHA considers that the consequences of classification under the Bill are so substantial as to require that assessments regarding classification be undertaken in respect of individual documents. The classification of a document renders it inaccessible to the public (without declassification) and carries criminal offences which involve the potential loss of liberty for those in possession of such information. It is therefore only reasonable that careful consideration be given to each and every document before it can be classified.

Accordingly, the power to classify categories of documents in clauses 7(1) and 13(5) should be removed and a requirement to individually consider information in respect of classification should be inserted.

Presumption of classification
Clause 13(6) provides that members of the security services who by the nature of their work deal with state information that *may* fall within the ambit of the Bill *must* classify that information (emphasis added). The term 'must' requires that all such information dealt with by those employees be classified as confidential, secret or top secret. It is not open to those employees to determine that none of the classification criteria apply and therefore the document does not require classification. A presumption of classification is therefore created.

Information classified in that manner will remain classified (clause 13(8)) until reviewed by the head of the organ of state who may either confirm the classification or declassify the information (clause 13(7)). There is no timeline for such a review to take place and accordingly the original classification, based on a requirement to classify, may remain in place for a substantive period, foreseeably until the 10 year review of such information occurs.

A presumption of classification in the context of the consequences of classification already discussed above is unreasonable. Furthermore, such a requirement would potentially be in conflict with clause 14, which sets out the conditions for classification. A member of the security services may consider that a document does not meet the conditions for classification in the Bill, while at the same time being required to classify the document under clause 13(6).

The word 'must' in clause 13(6) should therefore be changed to 'may' in order to ensure employees of the security service can exercise discretion based on the conditions for classification. Furthermore, a period within which a review of the information for the purpose of confirmation of classification must be undertaken should be inserted.

Reasons for classification
Clause 14(2)(d)(i) of the Bill requires that information be classified only when there is a clear, justifiable and legitimate need to do so. There are a number of instances in the Bill where the classification status of a document may be reviewed – by a superior (clause 13(8)), on a periodic basis (clause 18), on receiving a request for access to the document or an appeal related thereto (clauses 19, 31 and 32), or by the classification review panel (clause 21).

In order for the reviewer to determine whether a document was properly classified and accordingly whether there was a clear, justifiable and legitimate need to classify the document, the reviewer will need to consider the reasons of the original classifier. However, currently the Bill creates no obligation on the person classifying information to record their reasons for doing so. Without having to provide reasons for classification officials will not be able to be held accountable to their superiors and the review panel and courts will not be able to properly determine whether a classification was improper.

A requirement to record the reasons for classification, specifically how the information satisfies the demonstrable harm criteria in respect of the selected classification level (clause 12), should therefore be inserted.

<u>Review of classification</u>
Clause 18 of the Bill requires organs of state with the power to classify information to review that information. The clause is entitled 'regular reviews of classified information'. However, the substantive provisions require that a review of classification is undertaken only every 10 years.

Given the enormous impact that the classification of information will have on the public's right of access to that information and the criminalisation of conduct relating to that information, reviewing the classification status of information every 10 years cannot be sufficient. It is suggested that requiring such reviews to be undertaken every 5 years would strike a more appropriate balance between the resource implications of such a review and the consequences that result from the classification of the information.

Effect of the Bill on PAIA

Relationship between national security and PAIA

The Bill seems to have been prepared with little regard to or understanding of role the that PAIA plays in restricting access to information that relates to national security, international relations and the protection of individuals from harm.

Section 41(1) of PAIA provides that access to a record may be refused where its disclosure:

(a)could reasonably be expected to cause prejudice to –

(i) the defence of the Republic;

(ii) the security of the Republic; or

(iii) subject to subsection (3), the international relations of the Republic; or

(b)would reveal information –

(i) supplied in confidence by or on behalf of another state or an international organisation;

(ii) supplied by or on behalf of the Republic to another state or an international organisation in terms of an arrangement or international agreement, contemplated in section 231 of the Constitution, with that state or organisation which requires the information to be held in confidence; or

(iii) required to be held in confidence by an international agreement or customary international law contemplated in section 231 or 232, respectively, of the Constitution.

Further specifics about what may fall within section 41(1) are provided in subsequent subsections within PAIA.

Given that such information is already protected under PAIA, much of what the Bill sets out to do has already been achieved through PAIA and the Bill is therefore unnecessarily repetitive and seeks to extend the operation of PAIA without providing justification (see further discussion below on the issue of extending the operation of PAIA).

The preamble to the Bill includes the following statements:

Acknowledging that the right of access to any information held by the State may be restricted when necessary for reasons of national security.

...

Aiming to promote the free flow of information within an open and democratic society without compromising the national security of the Republic.

Those matters are both already achieved in PAIA, which was enacted with the purpose of placing reasonable restrictions on the right to information provided in the constitution, including on the basis of national security. Without evidence or merely even a suggestion as to how PAIA has proved inadequate in doing so it is unacceptable for the government to now seek to extend that protection through this Bill.

Similarly a number of the stated objectives of the Bill also overlap with those matters already addressed and achieved under PAIA. The objects of the Bill include to:

(b) promote transparency and accountability in governance while recognising that state information may be protected from disclosure in order to safeguard the national security of the Republic;

(c) establish general principles in terms of which state information may be made available or accessible or protected in a constitutional democracy;

(d) provide for a thorough and methodical approach to the determination of which state information may be protected;

...

(h) create a system for the review of ... requests for access to classified information...

The extensive overlap between the Bill and PAIA in terms of substantive provisions is perhaps most evident in an examination of clause 14(3) of the Bill. That provision sets out circumstances that may be considered when determining whether to classify a document. When each of the matters is examined against the grounds for refusing access to information in PAIA, it is clear that PAIA would protect the release of the information in every circumstance listed. The circumstances listed in clauses 14(3)(a) to 14(3)(e) of the Bill would all fall within the exemption from release of information in section 41 of PAIA. The circumstance listed in clause 14(3)(f) of the Bill would fall within the exemption from the release of information in section 38 of PAIA, which requires a public body to refuse access to a record if its disclosure could reasonably be expected to endanger the life or physical safety of an individual.

The application of the Bill to requests for access to information is therefore unnecessary in the context of the existing restriction on the right to information in PAIA. It is therefore SAHA's suggestion that all elements of the Bill which relate to the disclosure of classified information be deleted and matters related thereto continue to be dealt with under PAIA. In the event that the NCOP does not accept that submission SAHA has highlighted below specific problems with the disclosure procedure in the Bill and suggested amendments.

Bill overrides PAIA

Section 5 of PAIA provides that:

> *"This Act applies to the exclusion of any provision of other legislation that –*
> *(a) prohibits or restricts the disclosure of a record of a public body or private body; and*
> *(b) is materially inconsistent with an object or a specific provision of this Act."*

Therefore, PAIA currently stands as the authoritative legislation in determining restrictions on the right of access to information in South Africa.

The Bill proposes to amend that position. Clause 1(4) of the Bill provides that:

> *"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 provision ensures that restrictions on access to information within the Bill prevail over the release of information under PAIA.

SAHA notes that there has been some suggestion by government representatives that PAIA does not regulate 'classified' information and, as such, clause 1(4) of the Bill will have no affect on PAIA. However, respectfully, that interpretation is based on a misunderstanding of PAIA. PAIA regulates access to records. The term 'record' is defined in PAIA to include all records in the possession or under the control of the information holder regardless of form or medium. Therefore, in the absence of an express exemption, classified documents must fall within the definition of a record and therefore the release of those records is regulated by PAIA.

SAHA's interpretation is consistent with the current operation of PAIA. Many previously classified documents have been released to SAHA on the basis of a request for access under PAIA. Though classified documents are currently declassified in accordance with the MISS guidelines prior to release, the position concerning the right of access is determined under PAIA. That is, a classified record must be declassified and released if it cannot lawfully be refused in accordance with an exemption ground in PAIA.

Furthermore, the interpretation favoured by some government representatives ignores that the drafters of the Bill recognised the need to make express reference to section 5 of PAIA, evidencing that the drafters envision a conflict arising between the two laws.

Therefore, the correct legal interpretation must be that should the Bill become law, restrictions on the release of information under the Bill will apply even where the provisions of PAIA would require that information to be released.

Furthermore, it is arguable that any procedural inconsistencies between PAIA and the Bill would be determined in favour of the provisions under the Bill. The reference in clause 1(4) of the Bill to the 'regulation' of access to classified information is likely to be interpreted to include the process applicable in respect of access to classified information. Therefore, the process in the Bill will also 'prevail' where there is a conflict.

In light of this analysis there are two key areas of concern where the Bill will have a substantial and negative effect on the right to information under PAIA – by allowing information holders to refuse access to information merely because a record is classified and by changing the process for requesting access to information.

Clause 1(4) should therefore be removed and the Bill should be aligned with PAIA so that requests for access to classified information continue to be dealt with under PAIA.

<u>New ground of refusal – mere classification of a record is sufficient to refuse access</u>

Chapter 4 of Part 2 of PAIA sets out an exhaustive list of grounds on which public bodies may refuse a requester access to information. In refusing access on one of those grounds the public body must establish that the relevant criteria for refusal exist and provide reasons to the requester explaining those grounds.

The Bill extends the restriction on the constitutional right of access to information by allowing access to information to be refused merely on the basis that the requested record is classified. Clause 34(2) of the Bill expressly states that "*unless ordered by a court, no classified information may be made available to the public until such state information has been declassified".* This operates in conjunction with clause 19 of the Bill, which establishes a process for considering the declassification of a record on receipt of a request for access to that record.

The Bill therefore effectively inserts a new ground for refusal into PAIA, allowing access to records to be refused merely on the basis of their status as a classified document.

SAHA has been unable to identify any discussion or document where the need for such an additional ground for refusing access to information is contended by the government. Nor have information officers implementing PAIA identified to SAHA that the current grounds for refusal are insufficient to protect the national security interests of the state. In fact, section 41 of PAIA provides an extensive list of circumstances in which an information holder may refuse a requester access to information on the basis that it may prejudice the defence, security or international relations of South Africa. The decision to extend the protection of national security documents to encompass any document on the basis of its classification therefore appears to have been taken absent any evidence of current inadequacies in the protection of those documents and without meaningful debate.

In order for a restriction on a constitutional right to be valid it must be reasonable and justifiable (see section 36 of the Constitution). The failure by government to identify the inadequacies in the national security protections currently afforded under the less restrictive limitation on the right to information in PAIA and the unreasonably broad definition of national security in the Bill, in SAHA's view, render the restriction on the right of access to information proposed in the Bill unconstitutional.

<u>Process for obtaining access to classified documents</u>

Time for responding to a request

Where a person makes a request for access to information, section 25 of PAIA requires that the organ of state determine whether to grant access and inform the requester of their decision as soon as reasonably possible, but in any event within 30 days after receipt of the request.

Clause 19(6) of the Bill provides that where a person requests access to classified information the organ of state must determine whether to declassify the information 'within a reasonable time' (with the exception of where the release of the record satisfies the public interest override, in which case it must be determined within either 14 or 30 days, depending on the circumstances).

There is no indication within the Bill what may constitute a 'reasonable time' in respect of a declassification decision. However, the express mention of a 30 day time period for response within the provision addressing the release of information in the public interest, suggests that a 'reasonable time' would be greater than 30 days.

As outlined above, the Bill overrides PAIA to the extent of inconsistency. Therefore, clause 19(6) operates to extend the time for responding to a request for access to information under PAIA for an indeterminate period where the request relates to access to classified information.

The decision to extend the time for responding to a request under PAIA in these circumstances is concerning. The value of information is often time-bound and therefore any extension to the period of time for response may impact on the worth of that information to the requester. Furthermore, the current period of time for responding to a request in South Africa, 30 days, is already out of step with growing international best practice. For example, the recently passed Nigerian access to information law allows information holders only 7 days to respond to a request.

It is worthy of note that a Minister is required to determine an appeal based on a refusal to grant access to information within 30 days under the Bill (see clause 31(3)).

Of further concern in respect of the time provided to an organ of state for responding to a request is clause 19(5) of the Bill. That clause seems to suggest that a court may condone the non-observance by an organ of state with the 14 day time frame for responding to a request for a record which evidences an imminent and serious public safety or environmental risk.

This suggests that where an organ of state failed to provide a record of the nature indicated within the 14 days provided under the Bill, the requester would be forced to bring an urgent application to court seeking an order for the immediate provision of the information. At that time it would be open to the court to condone the failure by the organ of state to provide the information within the 14 day period, if good cause were shown. This places an unreasonable burden on the requester in an environment where court as an avenue of appeal has already proved out of the reach of most South Africans.

Statements made by representatives of the state security department at the public hearing in Sharpville on 14 February indicated that the intention of clause 19(5) is actually to allow a requester to apply to the court for urgent access to information which relates to an imminent and serious public safety or environmental risk (i.e. apply for access to be granted in less than 14 days). That is not the outcome that is achieved by the current drafting of the provision.

A requirement to determine requests for information within a 30 day period should therefore be inserted. Clause 19(5) should also be amended so that it does not allow the court to condone a late response from an organ of state, but rather allows a requester to apply to the court for urgent access to information.

Provision of reasons for refusing access

The Bill does not require organs of state to provide reasons for refusing to declassify a record. Accordingly, the Bill makes no provision for a requester refused access to information on the basis of its classification to receive reasons from the organ of state for that decision. It is unclear whether the requirement to provide reasons for refusal in the context of section 25(3) of PAIA will apply to a decision to refuse access to information on the basis that it is classified. Specifically, it is unclear whether the organ of state would need to provide reasons establishing the demonstrable harm criteria for the classification of a document (see clause 12 of the Bill). The Bill does not expressly

remove the obligation on the organ of state to provide reasons for the classification of a record, it is simply silent on the issue. It is therefore arguable that no direct conflict arises between PAIA and the Bill in this respect, in which case the obligation to provide reasons under PAIA would remain, even where access was refused on the basis of the classification of a record. However, the issue is unclear and a requirement to provide reasons should be inserted in the Bill for the purpose of clarity.

Without the provision of reasons for refusing to declassify information and provide access thereto it is difficult to anticipate how a requester could exercise their right to appeal to the Minister (clause 31), as it would be very difficult to make out grounds for appeal in the absence of knowledge as to why the initial request was refused.

It is worthy of note that if a request for access to information is refused by the Minister on appeal, the Minister is obligated to provide reasons for the refusal (clause 31(3)).

Appealing to the Minister
Clause 31(1) of the Bill allows a person who has been refused access to information under the Bill to appeal the decision to the Minister. In order to have been refused access to information a decision must have been made by the organ of state to which the original request for access was made. No provision is made in the Bill for circumstances where the organ of state fails to respond to the request for access. This would allow an organ of state to deny a requester the right to appeal simply by failing to answer the original request for information.

PAIA currently deals with a failure to respond by providing that the relevant body will have been deemed to have refused the requester access to information in the event that the body does not respond to a request within the statutory time frame. This provision is essential given the current failure of bodies to comply with their access to information obligations. Data collected by the PAIA Civil Society Network[1] from August 2010 to July 2011 revealed that 74% of the instances in which the Network was refused information was on the basis of the information holder's failure to respond to the request.

Accordingly, a provision must be inserted in the Bill that will allow a requester to appeal to the Minister in the event that the relevant organ of state fails to respond to a request for access. That provision should be linked to a timeline for responding to the original request.

The length of time allowed for lodging an appeal with the Minister is also inconsistent with PAIA. Clause 31(2) of the Bill requires a requester to lodge an appeal within 30 days of being refused access to classified information. Section 75 of PAIA allows a requester that has been refused access to information 60 days in which to apply to the Minister. Absent a valid reason for shortening the timeframe for lodging an appeal to the Minister in respect of classified information, clause 31(2) of the Bill should be amended to 60 days to ensure consistency with PAIA.

Lack of an accessible independent review mechanism
Clause 20 of the Bill establishes the Classification Review Panel (the Panel). One of the functions of the Panel is to review and oversee status reviews, classifications and declassifications of records (clause 21(1)(a)).

To ensure that the Panel is able to adequately perform its functions, provision has been made within the Bill to ensure that there is substantial expertise on the Panel. Specifically, clause 22(5) of the Bill provides that the Panel must consist of at least one member with expertise in the Constitution and the law, one member with knowledge and experience of national security matters and one member with knowledge and experience of archive related matters.

[1] The PAIA Civil Society Network is an umbrella body of organisations working to advance the right of access to information. The member organisations are committed to improving the implementation and usage of PAIA, raising awareness about the right amongst citizens and working with bodies subject to PAIA to improve understanding.

Despite the establishment of an independent expert body with functions in respect of declassification, no right is established in the Bill for requesters denied access to information on the basis of its classification to apply to the Panel for a review of a decision not to declassify information. Appeal rights are limited to an administrative appeal to the relevant Minister and judicial review.

While the appeal rights provided are consistent with those afforded to requesters of information from public bodies under PAIA, it has long been argued by civil society that the appeal rights provided under PAIA are inadequate for the full realisation of the right to information.

Data collected by the PAIA Civil Society Network from August 2010 to July 2011 demonstrates that the right of internal appeal to the political head of the same body that originally refused access to information is rarely effective in reversing a decision. During the stated period, members of the network lodged 28 internal appeals in response to 102 refused applications for information. Of those 28 applications, only 5 resulted in the release of information to the requester. More significantly, in 21 instances the Minister or other relevant party failed to even respond to the appeal.

Currently, where an internal appeal under PAIA is refused (or not responded to) the only available option for requesters is to make an application to court. However, the very small number of cases in which court action has been pursued, despite the high level of refusals to requests for information, evidences the inaccessibility of court for most South Africans and civil society organisations. The data collected by the PAIA Civil Society Network, referred to above, indicates that no member organisations filed court applications for the release of information during the assessment period, despite access being refused in 60 per cent of cases.

The repeated failure of the appeal mechanisms under PAIA have long been recognised by civil society organisations who have called for the establishment of an information commissioner, or similar body, that would provide for a less expensive, flexible and timely resolution of PAIA disputes by an independent, skilled arbiter. The failure to recognise the opportunity presented by the Bill to empower the Panel to fulfil such a role in respect of disputes over the release of classified information signifies a lost opportunity. Accordingly, an avenue of appeal to the Classification Review Panel should be inserted for requesters refused access to information.

Public interest override

Section 46 of PAIA obliges public bodies to release information to a requester, where that information could otherwise be refused under the Act, if the release of the information is in the public interest. However, the threshold of the public interest test established in the Act is so high as to render it almost entirely useless.

In order for a record to be released in the public interest PAIA requires that:

(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 release of information in the public interest is therefore limited to records which involve either of the circumstances in subsection (i) or (ii); a contravention of, or failure to comply with, the law or an imminent and serious public safety or environmental risk.

There are therefore very few circumstances in which PAIA allows the release of information in the public interest. Data collected by the PAIA Civil Society Network from August 2010 to July 2011 shows that despite members of the Network being refused access to information in 102 instances during that period, the public interest override was not once applied in favour of the requester.

The high threshold of the public interest test in PAIA does not accord with international best practice. Particularly significant is that both the Ethiopian and Liberian access to information laws allow the release of information despite the applicability of an exemption where the public interest in the release of the information outweighs the harm that would be caused by release. The application of the test is not limited to circumstances which involve a contravention of, or failure to comply with, the law or an imminent and serious public safety or environmental risk. The model access to information law for African Union member states currently being developed by the African Special Rapportuer for Freedom of Expression and Access to Information is also more favourable to the requester than PAIA, reflecting a similar position to the Ethiopian and Liberian laws.

Unfortunately, despite the problems with the public interest override in PAIA, the same test has been inserted verbatim into the Bill. The Bill requires an organ of state to review the classification status of a record where a person requests access to the classified document (clause 19). The record may only be released to the requester if a decision is made to declassify the record.

In assessing the classification status of the record the Bill requires the organ of state to assess the public interest in the record, requiring declassification and release if the relevant public interest threshold is met. The applicable public interest threshold is identical to that in PAIA. It is therefore unlikely that the public interest clause in the Bill will provide any significant benefit to citizens in ensuring the Bill does not restrict access to records, the release of which would be in the public interest.

Clause 19(3) should therefore be redrafted so that the organ of state must declassify information and grant the request for access to the information if the public interest in the disclosure of the state information clearly outweighs the harm that will arise from the disclosure.

Criminal offences

Unreasonable burden on members of the public to guard classified information

Government officials will be afforded the opportunity to be trained in the operation of the Bill and the requirements in relation to the protection of information. It has been evident at the public hearings hosted by the NCOP on the Bill that many members of the public are not aware of the content of the Bill or even aware of its existence. Given that there is no obligation in the Bill for government to inform members of the public of its content and train them in respect of the protection of information, it may be assumed that many citizens will remain unfamiliar with the content of the Bill even should it become law.

In this context the disproportionate obligations placed on government officials and members of the public in respect of the protection of information are entirely unreasonable.

Clause 48 provides that an official of an organ of state who wilfully or in a grossly negligent manner fails to comply with the provisions of the Bill may be subject to a fine or to imprisonment for up to 2 years.

Clause 46 provides that people (government officials) who unlawfully and intentionally destroy, remove, alter or erase valuable information may be subject to a fine or imprisonment of up to 3 years.

These measures for dealing with officials that don't comply with the Bill or deal unlawfully with valuable information must be contrasted against the obligations placed on the public who may come into possession of classified documents or documents that relate to a state security matter.

Clauses 15 and 44 provide that a person who comes into possession of a classified document must return it to the South African Police Service. If they do not they may be subject to a fine or imprisonment of up to 5 years. That such an offence applies in a country where many people are unlikely to be aware of the obligation, have an inherent fear of the police service based on the experiences endured under the apartheid government or where such an action may result in the

incrimination of a family member or friend who gave them the document, the provision is wholly unreasonable. It becomes even more unreasonable when one considers that the person may be subject to such harsh penalties even if they do not share the document with anyone and there are no defences available to them to explain their actions (discussed further below).

Clause 49 criminalises conduct in relation to the possession of information that constitutes a state security matter. As discussed above, the definition of state security matter is much broader than may be reasonably required for the protection of national security and those matters that properly relate to national security within the definition are adequately dealt with elsewhere. Accordingly, all matters related to the definition of state security matter, including clause 49 should be deleted.

In the event that the NCOP does not determine to delete all references to state security matters within the Bill then the unreasonable nature of clause 49 must be examined. This clause criminalises, amongst other things, the conduct of a member of the public who has possession of a document which relates to a state security matter and retains the document or fails to take proper care of the document. The applicable penalty is imprisonment of up to 10 years. No option of a fine is provided.

Given that such documents need not even be marked as classified under the Bill there is an even greater possibility that someone who comes into the possession of the documents will not know the consequences of their failure to deal with the documents consistently with the requirements of the legislation. Furthermore, as with the provisions in relation to failing to return classified information to SAPS, the penalties apply even when the person does not share the document with anyone and there are no defences available to the person to explain their action. The offence becomes ridiculous when the broad definition of a state security matter is applied – the result is that a member of the public who retains a copy of a contract between the State Security Agency and the company that cleans the agency's building could be jailed for 10 years.

Placing such high obligations on members of the public who will receive no training in the operation of the Bill and consequently their obligations under it, and indeed may not even be aware of the Bill is entirely unreasonable. When viewed in the context of the comparatively light sentences placed on government officials the provisions become even more unfair and indefensible.

Clauses 15, 44 and 49 should therefore be deleted.

Requisite intent

Clauses 36, 37 and 38 create offences aimed at safeguarding information from foreign states and those engaged in hostile activities. The offences carry very serious penalties ranging from 3 to 25 years in prison. Offences of this nature should be required to carry an intention to commit the prohibited act. For example, in the case of the offence of espionage in clause 36 of the Bill, it ought to be demonstrated that the person knew that giving the classified information to the foreign state would directly or indirectly benefit that state.

Currently these offences do not require actual knowledge that the prohibited harm would result. They allow conviction on the basis that the person 'ought reasonably to have known' that the harm would result. It is therefore not necessary for the state to prove that the individual accused knew that the harm would result, but only that a reasonable person in their position would have known.

Given the severity of the sentences attached to this action and the very nature of espionage offences and the like, the current threshold in the provisions is too low. Actual intent and knowledge must be demonstrated. Accordingly the words 'ought reasonably to have known' should be deleted from all three clauses.

Inadequate protection of whistleblowers

Clause 43 of the Bill provides that any person who unlawfully and intentionally discloses classified information in contravention of the Bill may be fined or imprisoned for up to five years unless their action was authorised or protected under another law, including the Protected Disclosures Act 2000.

There are several problems with this clause and the limited protection it affords to whistleblowers. Firstly, the Protected Disclosures Act applies only to employees and not to other persons that may come into possession of classified information that exposes wrongdoing. Such persons would therefore not be protected by this provision.

Secondly, the provision creates a reverse onus of proof, requiring the accused to prove to the court that their action was protected under the Protected Disclosures Act, rather than the ordinary burden of proof which would require the prosecution to prove that the disclosure was not protected.

Thirdly, the protection is limited to the offence in clause 43. It would not prohibit prosecution of the individual under one of the other provisions. For example, the person may still be prosecuted under clause 44 for failing to return the information to SAPS, an offence that carries a potential five year sentence.

Lastly, the purpose of whistleblowing is to expose wrongdoing. It is therefore most effective when the wrongdoing is made known publicly. However, if a whistleblower were to inform a reporter of the wrongdoing evidenced in classified information and the reported published the wrongdoing, the reporter could be criminally prosecuted under the Bill.

New provisions regarding whistleblowing that rectify these concerns must be inserted into the Bill.

No defence available to accused

Despite the harsh and unreasonable criminal provisions in the Bill that apply to ordinary citizens who should ordinarily bear no obligation for the safeguarding of the state's secrets beyond acts of espionage and similar acts of malicious intent, the Bill does not allow members of the public charged with criminal offences under the Bill to offer any explanation of their actions by way of a defence. This omission is entirely unjust and a number of defences should be inserted into the Bill.

Improper classification

Firstly, it should be a defence to an offence involving classified information that the information has been improperly classified. Clauses 12 and 14 of the Bill set out the criteria upon which information must be classified. Clause 47 of the Bill sets out circumstances in which the improper classification of information will constitute an offence.

Despite these provisions, it is not open to a person accused of retaining or disclosing classified information to interrogate the appropriateness of the classification. Accordingly, a person may still be prosecuted and convicted for disclosing information that has been illegally classified on the basis that it conceals a breach of the law, for example it evidences corruption.

That someone may be convicted and imprisoned based on their dealings with information that has been classified inconsistently with the requirements of the Bill will certainly lead to injustices. Therefore a provision allowing an accused to interrogate the legality of the classification of the document must be inserted.

In order to further safeguard against the prosecution and potential conviction of a person's dealings with incorrectly classified information, the Classification Review Panel should be required to undertake a review of any classified information prior to the arrest and prosecution of someone in respect of that information.

The panel is appointed for the purpose of providing expertise in matters of classification and reviewing decisions of organs of state in respect of classification. However, as it will not be possible for the panel to review all classified information, it is possible that a prosecution in respect of conduct relating to classified information may occur without the panel having reviewed the classification of that information. In those circumstances the expertise of the panel in reviewing the classification

should be invoked before any arrest or prosecution is undertaken. A provision to that effect should be inserted in the Bill.

Public domain defence
The purpose of the classification of information is to ensure its secrecy. Once information is no longer secret, the purpose of the classification no longer exists. Accordingly, once information is in the public domain it should lose its classified status.

Currently information classified under the Bill remains classified irrespective of how broadly it may be available in the public arena. This means that anyone in possession of classified information, no matter how widely the information has been distributed, may be prosecuted and imprisoned for possessing that information.

The circumstances that may flow from the operation of the Bill in this manner are farcical. For example, if a reporter at a newspaper came into possession of classified information and determined to publish that information that reporter and the editor of the paper would be subject to the criminal provisions under the Bill. However, the criminal provisions would not only apply to those people. Any member of the public who picked up a copy of the newspaper would be in possession of the classified information and if they failed to return the paper to SAPS they could be prosecuted and imprisoned for up to 5 years. The consequences of such a scenario would place an unreasonable burden on the police, prosecutors and the courts. There must be a point at which classified information is so broadly within the public domain that the purpose of its classification, to keep the information secret, ceases to exist and accordingly it loses its classification status.

Public interest defence
A public interest defence has been the subject of much public debate in respect of this Bill. While SAHA acknowledges that such a defence would be highly unusual, based on the current drafting of the Bill a public interest defence is essential to ensure the reasonable and fair application of classification provisions and criminal sanctions.

However, in the event that the amendments to the Bill suggested in this submission, particularly those in relation to the type of information that may be classified, the process for classifying information and the suggested amendments to the criminal provisions are made, then SAHA does not consider the inclusion of a public interest defence would be essential.

A public interest defence would allow those people charged with a criminal offence to defend their actions in respect of retention, disclosure, publication, etc of classified information on the basis that they did so in the public interest.

While it has been government's position that the term public interest is not sufficiently certain to constitute a basis for assessment, the term already exists in the Bill. Clause 19 of the Bill requires an assessment of the public interest in the context of declassification of information. The identification of a national key point, under the National Key Point Act (incorporated into the Bill by reference) also includes an assessment of the public interest. Assessments of what is in the public interest are therefore already required to be made by officials and the courts.

A public interest defence could therefore take on the nature of the suggested test in respect of the public interest override. That is, did the public interest in the retention, disclosure, publication, etc of the information outweigh the harm that the classification of the document and the criminalisation of its release sought to prevent.

Other
Clause 17 of the Bill refers to section 11(2) of the National Archives of South Africa Act 1996. That section relates to the transfer of information from public bodies to an archive repository, not public access to information. The relevant section of the Act is 12(1). The appropriate amendment should therefore be made.

Clause 54 of the Bill allows the Minister to make regulations. The regulations authorised by sub-clauses (3) and (4) both require public consultation prior to adoption. However, there is no consultation requirement in respect of regulations of the nature referred to in sub-clause (1). Those regulations deal with substantive as well as procedural matters and therefore a requirement for public consultation should be inserted.

Conclusion

If the Bill is passed in its current form it will represent an erosion of the right to information in South Africa without justification and based on broad criteria whose relationship to national security is vague at best. Adequate protections for information relating to national security, defence and international relations are already provided under PAIA and accordingly the provisions of the Bill relating to access to information should be removed and access to information should continue to be regulated by PAIA. Alternatively, the provisions of the Bill must be brought in line with PAIA so that the right to information is protected. A failure to do so will render the Bill unconstitutional.

Furthermore, criminal sanctions applicable to members of the public must be reviewed to take proper account of where the responsibility for protecting classified information should properly fall. Defences should be inserted to ensure that unjust outcomes do not result.

Should you require further written or oral submissions on these issues SAHA would be happy to assist. Please contact Tammy O'Connor on the details below.

Prepared by: Tammy O'Connor
Advocacy and Training Outreach Officer
Freedom of Information Programme
South African History Archive
Ph: 011 717 1941
Fax: 011 717 1946
Email: tammy@saha.org.za

**Some of the content of this submission was originally prepared by the author on behalf of the PAIA Civil Society Network.*