RECOMMENDATIONS IN RESPECT OF THE PROTECTION OF INFORMATION BILL

1. The dramatic surgery that the Protection of Information Bill has undergone during the course of the Parliamentary process has meant that it is now close to being an official secrets law of more or less conventional scope. Such a law must strike a balance between, on the one hand, the principle of state security and the necessity to protect the inhabitants of the country against harm, and on the other hand, the countervailing principles of freedom of information, freedom of the media and the constitutional obligations of governmental openness and transparency. Acknowledging the difficulty of striking this balance, we offer the following comments and recommendations on the current draft of the Bill.

Correction of the limited scope of the public-interest override in the PAIA

2. The Protection of Information Bill is subject to the PAIA. This means that the Bill in effect incorporates the PAIA's *public-interest override* (section 46 of the PAIA). This means that a PAIA request for classified information is dealt with in terms of the PAIA. Even if there is a PAIA ground of refusal applicable to a particular record, the grounds of refusal are subject to an override in the public interest. As currently formulated, a record must be disclosed if disclosure "would reveal evidence of … a substantial contravention of, or failure to comply with the law; or … an imminent and serious public safety or environmental risk" and the public interest in disclosure outweighs the reasons for non-disclosure.

3. Although an important source of flexibility in the Bill, the effectiveness of this public-interest override is limited by the unreasonably high threshold that the PAIA imposes. This is a major and longstanding flaw in the PAIA. The scope of the override is simply too narrow and it is arguably unconstitutional. Our recommendation is that the committee considers effecting a consequential amendment to the PAIA that will correct this flaw and also provide an important recalibration of the Bill itself.[1]

Restoration of the 2008 wording of the penalties clauses

4. There are significant drafting changes between the 2008 and 2010 versions of the espionage and hostile activity offences as well as some of the other offences in the Bill. Further, the offence of disclosure of a state security matter (clause 43) is a new feature of the 2010 Bill. These drafting changes reflect two fundamentally different approaches to the criminalization of the use and disclosure of classified information. In terms of the current law (ie, the Protection of Information Act 1982 and the MISS), the criminal offences relating to the use and possession of classified information are regulatory offences. This means that criminalization attaches to the disclosure, or use, or possession of the particular information that has been classified. It is essentially the action of accessing the information that is criminalized. The 2008 Bill took a different approach to criminalization. Its approach was to criminalize the harm caused by disclosure of classified information rather than the fact that classified information had been disclosed. Thus, for instance, the action of communicating information

[1] This would entail deleting subparagraph (a) of section 46 of the PAIA.

which may cause serious harm to the Republic was criminalized. Essentially, the drafting style of the 2008 Bill incorporated a harm test within the substance of the criminal offences. The 2010 version of the Information Bill has reverted to the pre-2008 drafting style, ie to the definition of the offences as regulatory offences.

5. This drafting style is appropriate for relatively minor (e.g. "regulatory" or "non-compliance") offences against government information security rather than for major criminal offences against the security of the state, such as espionage.

6. In our view, a return to the 2008 drafting style of the offences would represent a significant improvement upon the current draft Bill. The use of this substantive drafting style would allow accused persons to argue and attempt to demonstrate that they have in fact acted in a manner that protected rather than harmed the security of the state. This substantive drafting style thus puts the focus not on the mere access to classified information but rather on the actual and potential consequences of use of that classified information.

7. It is arguable that a return to the substantive drafting style of the 2008 Bill would also have much the same benefits as the express inclusion of a public interest defence, without risking misuse of an explicit public interest defence. Unlike the inclusion of an explicit public interest defence, a return to the substantive drafting style would not allow an accused person who had caused serious harm to the Republic to argue that this harm was offset by a public interest in disclosure. A return to the 2008 substantive drafting style thus may represent a middle way between the exclusion and

the inclusion of a public interest defence in relation to the criminal offences of the current draft Bill. However, we regard the inclusion of an explicit public interest defence as essential if no revision to the drafting style is effected.

8. It is unlikely however that a mere change of wording will cure the overreach of the current clause 43. It is recommended that the clause be deleted.

An opt-in regime for organs of state outside the state-security sector

9. The most recent amendments to the Bill have been aimed at achieving the fundamental shift of emphasis from a general state information-security law to a narrow official secrets law aimed at protecting information of significance to national security rather than information that is in the national interest. However, the scope of the Bill remains extremely broad, purporting to regulate all state information (clause 1), allowing classification at a non-secret level of "confidential" (clause 15(1)) and applying (unless exempted) to all organs of state (clause 3).

10. These scope provisions are at odds with the Bill in its current form. As indicated above, the deletion of chapter 5 removes the heart of the Bill's original information-security scope of application. Accordingly, consideration needs to be given to a consequent reconsideration of the organs of state on which the Bill's duties are imposed.

11. Our recommendation in this regard is that the definition of organs of state should distinguish between two categories of entity. Category A entities would be those

falling into the state-security sector: defence, police, intelligence etc. Category B entities would be the remaining organs of state. Category A entities would then be subject to the Bill but would be able to opt out of its duties if they were not in fact in possession of any classifiable information. Category B entities would not be automatically subject to the Act but would be able to opt in if they found themselves dealing with classifiable information.[2]

Automatic declassification

12. Clause 26 of the 2008 version of the Bill provided for automatic declassification of all pre-1994 classified information and all information more than 20 years old. This was a most progressive proposal. It is the only systematic way to deal with the over-classification of records that took place in terms of the previous information security and classification legislation. We recommend the restoration of this provision.

13. The current clause 20 is by contrast far too narrow, applying only to those records transferred to the National Archives in terms of the National Archives Act. This is a fraction of the records generated by the state and will result in most information simply remaining classified in perpetuity.

[2] Such a device might also be used to revive the Bill's deleted information security provisions. These could be a separate class of duties, imposed generally on all organs of state. The official secrets duties would be placed solely on category A entities.