Rhodes University on the Protection of State Information Bill:

Changes welcome, but the Bill still threatens academic freedom

Rhodes University notes the fact that Parliament has passed the Protection of State Information Bill, otherwise known as the Secrecy Bill, and the Bill now awaits President Zuma's signature.

The University welcomes the fact that the apartheid-era Protection of Information Act of 1982 is going to be repealed once the Bill comes into force, and also welcomes the changes made to the Bill by both houses of Parliament. The higher education sector, represented by Higher Education South Africa also made a written and oral submission to the National Council of Provinces on its concerns on the Bill and its implications for academic freedom.

The cumulative changes made to the Bill since its re-introduction to Parliament in 2010 has led to the Bill striking a more appropriate balance between national security, on the one hand, and the rights to freedom of expression and access to information on the other: rights which are dear to this University, as without them, academic work would become impossible.

The University welcomes the fact that the scope of the Bill has been limited largely to the Cabinet, the security cluster and their oversight services; it now includes a limited defence for disclosure of classified documents, and has narrowed the definition of national security and the criteria for classification of documents. The Bill has also largely excluded commercial information from its purview. The clause that allowed the Bill to override the Promotion of Access to Information Act on state security matters has also been removed, and Chapter Nine institutions can now receive classified information, which would have hampered their work if they were unable to.

However, some significant weaknesses still remain, which makes the University believe that the Bill still threatens academic and other freedoms. Although the definition of national security is much narrower than it was, it is still open-ended, which means that more issues could potentially be added to the definition. Furthermore, aspects of the definition remain vague and open to abuse, such as 'the exposure of a state security matter with the intention of undermining the constitutional order', and 'the exposure of economic, scientific or technological secrets vital to the Republic'. This is of particular concern to the University, as it is this sort of information that could be used to advance research. These definitional problems could well lead to over-classification of documents that should rightfully be in the public domain.

The Bill also contains general principles of state information, which are largely progressive statements recognising the need for openness and transparency in the security sector; however, these principles can still be trumped by 'national security', which means that there will be a presumption in favour of classification if there is uncertainty as to whether to classify a document or not. In other words, the classifiers' fall-back position will be to classify, rather than to declassify.

The Minister of State Security can still include other organs of state as organs that may implement the Bill if they show good cause, and if Parliament approves their inclusion, which means that the reach of the Bill could be expanded gradually. The Bill still gives heads of

organs of state the power to come up with policies, directives and categories for classifying, downgrading and declassifying state information and protection against alteration, destruction or loss of state information created, acquired or received by that organ of state. This creates uncertainty in the classification regime because - in spite of the proviso that these policies shouldn't be inconsistent with regulations or the constitution - given the large number of organs of state it is impossible to ensure uniformity and certainty in the access of information regime. Furthermore, since the organs of state are not obliged to consult members of the public before coming up with the policies, citizens would be unjustifiably denied the right to participate in decisions that affect them. The range of officials with the power to classify is also too broad, as it includes employees 'who by the nature of his or her work' deal with classified information.

The Bill still does not oblige those making classification decisions to give reasons for their decisions, which means that they cannot be held accountable for their decisions. Furthermore, if information forms part of a particular category of information that falls to be classified, then it will be classified whether it is sensitive or not, which is likely to result in over-classification. The Bill also retains a classification period of 20 years, which is too long and not in line with international best practice.

A further problem is that the Minister of State Security still adjudicates on classification and declassification decisions in other state departments, rather than an independent arbitrator, which – given the culture of secrecy prevailing in the intelligence services – is likely to skew decision-making towards secrecy and away from openness. Furthermore, the State Security Agency still monitors all organs of state for compliance with the Act, this may also incline the system towards greater secrecy, given the culture of secrecy that tends to pervade the intelligence community. This function should be left to an independent institution.

Furthermore, information that has been classified under constitutionally dubious laws, such as apartheid-era laws, will not be automatically declassified but will still be protected, which means that possession of, or disclosure of, apartheid era secrets can still be prosecuted under the law. No time limit has been set on the declassification of these documents, which means that potentially they could remain secret indefinitely: a particular concern for historical researchers. The body established to review classification (the Classification Review Panel) is not sufficiently independent and the simple possession of classified information appears to be illegal even pending a request for declassification and access.

The Bill still criminalises simple possession and disclosure of classified information, which means that the state's obligation to protect classified information has been transferred to society as a whole. The problem is compounded by the fact that the Bill still lacks a public domain defence, where a person who discloses classified information can argue that this does not constitute an offence if the information is already in the public domain. The public interest override is still narrow, as it applies only to information that reveals evidence of illegality, safety or environmental risks. The clause does not allow disclosure of information that may be in the public interest, but that may fall short of outright criminality, such as improper appointments within key state agencies or inappropriate policy decisions or use of state resources. A whistleblower, journalist or activist who discloses a classified record with the purpose of revealing corruption or other criminal activity may be prosecuted under the 'espionage' and other offences not covered by the public interest defence.

Furthermore the offences of ‘espionage’, ‘receiving state information unlawfully’ and ‘hostile activity’ could still be abused to punish researchers, journalists, whistleblowers and others who disclose classified information they believe to be in the public interest. Sentences are excessive: up to 25 years in the case of an espionage offence.

The cumulative effect of these remaining problems is likely to be that the Bill, once it is enacted, will result in a culture of over-classification in the security sector. Researchers that need access to documents that expose the inner workings of the security cluster, and its interface with society, may continue to be frustrated as the documents they seek are classified. They may also fear coming into the possession of classified documents, and as a result may shun researching the activities of the cluster, which could lead to knowledge being lost in this domain.

A secretive security cluster is dangerous, as it could allow all manner of abuses to take place in the name of protecting national security. Recent incidents involving the security cluster, such as the killing of mineworkers at Marikana, the killing and injuring of protestors during clashes with the police, the deaths of soldiers in the Central African Republic and the controversy around the disclosure of information about the upgrading of President Zuma’s residence in Nkandla (apparently a National Key Point), all suggest that the security cluster is a troubled institution and in need of public scrutiny. South Africa can ill-afford a security cluster that is embroiled in ongoing conflict with its own citizens. It is the role of universities to analyse the deeper processes at work in the state and society, and develop knowledge resources for the betterment of society. With a Bill such as this on the statute books, the University fears that it will be unable to play this role with regards to this most sensitive area of government, which we believe will be to the detriment of its students and, ultimately, society as a whole.